أطروحة الماجستير في القانون العام

بعنوان

"حجية التوقيع الإلكتروني في الإثبات"

(دراسة مقارنة)

إعداد

المقدم/ عبد الرحمن خلفان الخيال الحارثي

الشارقة 2019م

4342.620999 الحارثي، عبدالرحمن خلفان الخيال

• ح ع ح

• حجية التوقيع الالكتروني في الاثبات/ عبدالرحمن خلفان الخيال الحارثي - الشارقة، الامارات العربية المتحدة: مركز بحوث الشرطة، ٢٠١٩

• ص ؛ ٢٤ سم (مركز بحوث الشرطة ؛ ٢١٧)

يحتوي على مراجع

١- الانترنت - قوانين وتشريعات ٢- الحاسبات الالكترونيه - قوانين وتشريعات

٣- الاثبات (قانون) ٤- الجريمة والمجرمون - الامارات العربية المتحدة

أ- العنوان

ISBN 978-9948-36-359-0

تمت الفهرسة بمعرفة مكتبة الشارقة

مادة الإصدارات تعبر عن آراء كاتبيها
وليس بالضرورة عن رأي مركز بحوث الشرطة

حقوق الطبع محفوظة لشرطة الشارقة / مركز بحوث الشرطة

الطبعة الأولى 1441هـ – 2019م

ص. ب: 29 ، الشارقة – الإمارات العربية المتحدة

هاتف: 5945112 – 009716 براق: 5382013 – 009716

E-mail: prc@shjpolice.gov.ae Website : www.shjpolice.gov.ae

بسم الله الرحمن الرحيم

قال تعالى:

الذين آمنوا ولم يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون

سورة الأنعام / الآية (82)

التوجه الاستراتيجية لوزارة الداخلية
2017 - 2021م

- **الرؤيــة :**

أن تكون دولة الإمارات العربية المتحدة من أفضل دول العالم في تحقيق الأمن والسلامة.

- **الرسالـة :**

أن نعمل بفاعلية وكفاءة ولتعزيز جودة الحياة لمجتمع الإمارات من خلال تقديم خدمات الأمن والسلامة بطرق ذكية وبيئة محفزة للابتكار وذلك حفاظا على الأرواح والأعراض والممتلكات.

- **القيــم :**

1- العدالة. 2- العمل بروح الفريق. 3- التميز والابتكار.
4- حسـن التعامل. 5- النزاهة. 6- الولاء.
7- المواطنة الايجابية.

- **الأهداف الاستـراتيجية :**

1- تعزيز الأمن والأمان.
2- جعل الطرق أكثر أمنا.
3- تعزيز السلامة والحماية المدنية.
4- ضمان الجاهزية والاستعداد في مواجهة الأحداث.
5- تعزيز رضا المتعاملين بالخدمات المقدمة.
6- ضمان تقديم كافة الخدمات الإدارية وفق معايير الجودة والكفاءة والشفافية.
7- ترسيخ ثقافة الابتكار في بيئة العمل المؤسسي.

يقوم مركز بحوث شرطة الشارقة بإصدار ونشر سلسلة من الدراسات في مختلف مجالات العمل الأمني والشرطي.

شــروط النشـــر

1. الأصالة في مجال العلوم الشرطية والأمنية والتخصصات الأخرى ذات الصلة، وأن تكون الدراسة لم يسبق نشرها من قبل.

2. مراعاة قواعد وأصول البحث العلمي من حيث الأسلوب والنظرية والمنهج.

3. أن تتضمـن الدراسـة الرجـوع إلـى المصـادر العلميـة الحديثة.

4. أن تكتب الدراسة وتطبع بلغة عربية سليمة ويرفق معها ملخص باللغتين العربية والإنجليزية وألا يقل حجم الدراسة عن أربعين صفحة.

5. يلتزم الباحث بعدم إرسال دراسته إلى أي جهة أخرى للنشر حتى يصل إليه رد المركز وتعطى الأولوية للنشر حسب الأسبقية الزمنية للتحكيم.

6. لا يلتـزم المركز برد أصل الدراسة سـواء تـم نشــرها أم لا.

7. تخضع الدراسات للتحكيم وتقرر الهيئة العلمية المشرفة على الإصدارات صلاحية الدراسة للنشر بناء على رأي ثلاثة محكمين متخصصين.

هيئة التحرير المشرفة على إصدارات
مركز بحوث شرطة الشارقة :

• المشرف العام : اللواء / سيف محمد الزري الشامسي
قائد عام شرطة الشارقــة

• رئيس التحرير : العميد الدكتور / خالد حمد الحمادي
مدير إدارة مركز بحوث شرطة الشارقة

• مدير التحرير : المقدم / عبدالله محمــد المليــح
رئيس قسم البحث العلمي
بمركز بحوث شرطة الشارقة

• الإشراف التنفيذي : النقيب / علي محمد بن هندي
مدير فرع البحوث الأمنية
بمركز بحوث شرطة الشارقة

• الإشراف الفني : المساعد/ أحمد أمين الزرعوني

أعضـاء الهيئـة العلمية المشرفة على
إصدارات مركز بحوث شرطة الشارقة:

- المقدم/ عبدالله محمـد المليـح — رئيس قسم البحث العلمي بمركز بحوث شرطة الشارقة
- المقدم/ د. خليفة يوسف بالحاي — مكتب القائد العام
- المقدم/ د. عبدالله سيف الذباحي — مدير فرع الخدمات المساندة بمركز شرطة خورفكان الشامل
- الرائد/ د. جاسم بن جرش السويدي — مدير فرع التعليم الافتراضي بأكاديمية العلوم الشرطية بالشارقة
- الدكتور/ نواف وبدان الجشعمي — رئيس شعبة دراسات الجريمة بمركز بحوث شرطة الشارقة

تقديـــم

تمثل مناهج البحث العلمي السبيل الرئيسي لإقامة الحضارات واستباق الأمم. كما أنها تعد الأداة الأولى في تطويع تحديات الحاضر واستشراف المستقبل.

ويعد مركز بحوث شرطة الشارقة بالقيادة العامة لشرطة الشارقة أحد المراكز البحثية بالدولة والتي تتطلع بدور مهم في رصد كافة الظواهر الاجتماعية والأمنية وبحث أفضل الآليات للاستفادة من إيجابياتها ووأد سلبياتها لضمان استمرار ركب التنمية والتقدم ، كما يقوم المركز من خلال دراساته في مختلف جوانب الحياة الاجتماعية والقانونية والأمنية وبالتعاون والتنسيق مع المراكز البحثية الأخرى بالدولة وخارج الدولة بتقديم أفضل الحلول والمقترحات لكافة قضايا المجتمع.

وفي هذا الصدد تتعدد صور النشاط العلمي لمركز البحوث ما بين مؤتمرات وندوات وعقد دورات وحلقات ومحاضرات ومنشورات علمية ، وهو الأمر الذي يسهم بلا ريب في إثراء مجالات الفكر العلمي والأمني المختلفة وتقديم المشورة الفاعلة لمتخذي القرار وتوفير قاعدة علمية متميزة لكافة الباحثين والعاملين في مجالات العمل الاجتماعي والقانوني والأمني المختلفة للنهل منها وتقديم كل ما هو نافع ومفيد للحفاظ على مكتسبات المجتمع وأمنه.

والله ولي التوفيق،،،

اللواء / سيف محمد الزري الشامسي

قائد عام شرطة الشارقة

توطئـــة

في إطار تفعيل دور مراكز البحوث الأمنية ، يصدر مركز بحوث شرطة الشارقة مجموعة من الدراسات والبحوث في مجالات الأمن بمفهومه الشامل بهدف تكوين ثقافة أمنية لدى العاملين في الجهاز الشرطي، ودعم الدور المجتمعي في مجالات مكافحة الجريمة ، كما أنها وفي الوقت ذاته تمُد صاحب القرار الأمني بقاعدة بيانات علمية دقيقة تساعده في اتخاذ القرار السليم.

وتتضمن إصدارات عام 2019م عدداً من الدراسات والأبحاث المتميزة التي جاءت استجابة للتحديات الأمنية والمجتمعية وتصدياً للجرائم المستحدثة وملبية للتوجه الوطني والمؤسسي نحو التميز الاستراتيجي مواكبة للتطورات العالمية والمتمثلة في العولمة وإفرازاتها وتعالج قضايا أمنية وإدارية، بالإضافة إلى موضوعات قانونية واجتماعية.

وتتناول هذه الدراسة موضوع في غاية الأهمية خاصة في ظل انتشار الواسع للتكنولوجيا، إلا وهو مدى حجية التوقيع الالكتروني في الاثبات، وما يتعين على المشرع القيام به لمعالجة هذه المشكلة التي أصبحت واقعاً حتمياً.

نأمل أن تشكل هذه الدراسات بجانب الفعاليات العلمية التي يقدمها مركز بحوث الشرطة زاداً فكرياً ومعرفياً يعود بالنفع على كافة المواطنين والمقيمين في دولة الإمارات العربية المتحدة وفي أرجاء وطننا العربي والمهتمين والمختصين بهذا المجال.

العميد الدكتور / خالد حمد الحمادي

مدير إدارة مركز بحوث شرطة الشارقة

المحتويـــات

مستخلص 19
المقدمـــة 23
مشكلة الدراسة 25
تساؤلات الدراسة 26
أهداف الدراسة 26
منهج الدراسة 27
خطة الدراسة 27

المبحث التمهيدى: ماهية التوقيع الإلكتروني 29

المطلب الأول: تعريف التوقيع الإلكتروني 30
المطلب الثاني: خصائص التوقيع الإلكتروني وأهميته وصوره 38

الفصل الأول: القوة الفنية والثبوتية للتوقيع الإلكتروني 59

المبحث الأول: آلية تشفير التوقيع الإلكتروني 60
المبحث الثاني: طرق التحقق من سلامة الرسالة والمصادقة عليها 81

الفصل الثاني: شروط حجية التوقيع الإلكتروني وآثاره في الإثبات 113

المبحث الأول: شروط حجية التوقيع الإلكتروني 114
المبحث الثاني: آثار التوقيع الإلكتروني وتطبيقاته 134
المبحث الثاني: وظيفة التوقيع الإلكتروني ودوره في الإثبات 148

الخاتمـة 181

النتائــج 181

التوصيات 184

قائمة المصادر والمراجع 185

مستخلص

تتناول الدراسة موضوع حجية التوقيع الإلكتروني في الإثبات، دراسة في التشريع الإماراتي والتشريعات المقارنة والذي يعد من أهم الموضوعات المستحدثة التي تناولها فقهاء القانون في الوقت الراهن كأحد أهم البدائل المستحدثة للتوقيع التقليدي حيث أصبحت المعاملات الإلكترونية حقيقة قائمة في العالم المعاصر، وهي آخذه في التطور السريع ولكنها تواجه إشكالية تتعلق بالإثبات في وقت هي بحاجة إلى وسائل غير تلك التقليدية المتعارف عليها حتى تتماشى مع الحلول القانونية نتيجة الاتساع المذهل لحجم تلك التجارة والمعاملات كافة. وحيث أن التوقيع بشكل عام هو الوسيلة الأبرز للتعبير عن إرادة صاحبه وموافقته على مضمون السند، فإن التوقيع بشكله الإلكتروني قد يجعل المسألة في التشريعات التقليدية أكثر تعقيداً وذلك لغياب الوسائط المادية أو التقليدية التي يثبت عليها ، ولذلك فقد حظي بأهمية خاصة، فالكثير من التشريعات الحديثة سواءً كانت عالمية أو وطنية، عرّفت التوقيع الإلكتروني ونظمت أحكامه ولذلك كان لزاماً على الباحثين الاهتمام بدراسته، والتعرف على كل ما يتعلق به من منظومة الكترونية بهدف الوقوف على كيفية إثبات التصرفات القانونية التي تتم عبر الانترنت ، دون استخدام الأوراق التقليدية ومعرفة مدى حجية مخرجات هذه الوسائل في الإثبات، لاسيما وأن دولاً كثيرة ما زالت لم تنظم هذا الشأن بقواعد قانونية تنسجم مع خصوصيته، وحاجة المجتمع إليه، فبقيت مكتفية بما ورد من قواعد تقليدية أو عامة في الإثبات، و لذلك كان لا بد مع هذا الوضع من معرفة مدى حجية التوقيع الإلكتروني في الإثبات. وخلصت الدراسة إلى مجموعة من النتائج والتوصيات، أهمها إنّ الهدف من شهادة التصديق يتمثل في تأكيد صحة وقانونية البيانات الواردة في الشهادة، وأوصت بضرورة إدخال موظفي الجهات ذات العلاقة المباشرة بالتوقيع الإلكتروني في دورات تأهيلية تمكنهم من التعامل مع تلك الوسائل المستحدثة.

Evidentiary Value of Electronic Signature

حجية التوقيع الإلكتروني في الإثبات

This study deals with the topic of evidentiary value of electronic signature, a study on UAE's and comparative legislations. It is one of the most important new topics debated by jurists at the present time as a key, modern alternative to the traditional signature. This alternative is important as electronic transactions have become a reality in the modern world and are rapidly evolving. However, such transactions, given their impressive volume, are faced with a proof-related problem, and require unconventional means to conform with legal solutions. As signature in general is a major means of expressing the person's will and consent to the content of a document, electronic signature makes this even more complicated in traditional legislations owing to the lack of physical or traditional media of evidence. Thus, electronic signature received particular attention: numerous modern legislations, both internationally and nationally, have defined electronic signature and regulated relevant provisions. Researchers should, therefore, study electronic signature and get acquainted with all its aspects to come out with a way for proving the evidentiary value of electronic transactions, especially as many countries - satisfied with traditional or general rules of evidence - still have not regulated this matter with rules that are consistent with its nature, and with the need of society for it. Given that situation, determining the evidentiary value of electronic signature is imperative. Study sums up with a number of findings and recommendations; major among them is that the aim of attestation certificate is to verify the authenticity of information stated in the certificate as well as verifying authenticity of E-signature. Study also recommends the need to provide staff of entities directly concerned with electronic signature, with training courses so as to be able to handle such new methods.

المقدمة

تعدّ الكتابة دليلاً كاملاً إذا وقعت باعتبار أنّ هذا التوقيع يُعدّ العنصر الثاني من عناصر الدليل الكتابي المعدّ للإثبات، ودون التوقيع يفقد الدليل الكتابي حجيته، فقد كان التوقيع بدايةً يتم عن طريق الختم ثم أصبح يتم عن طريق الإمضاء بخط اليد باعتبار أن التوقيع عمل شخصي لا يقوم به إلا صاحبه لأنه يدلذ على تدخّله بصفة مباشرة وليس عن طريق النيابة عن شخص آخر.

وبفضل التطوّر التقني لوسائل المعلومات والاتصالات تحوّل المجتمع من مجتمع ورقيّ إلى مجتمع لا ورقي؛ أي: إلكتروني، إذ ظهر مستند للمعلومات يختلف جذريًا عن المستند الورقي التقليدي، ومن ثمّ بدأت المستندات الورقية الموقع عليها خطيًا تتراجع شيئًا فشيئًا في العمل ليحلّ محلّها –تدريجيًا– أنواع جديدة من المستندات تعتمد على دعامات غير ورقية تسمّى بالمحرّرات أو السندات الإلكترونية مصحوبة بتواقيع أطلق عليها التواقيع الإلكترونية.

لقد خضعت القواعد القانونية للتعاقد في النظم المقارنة إلى عملية تقييم في ضوء مفرزات تقنية المعلومات وتحدّياتها، وذلك من أجل بيان مدى إمكانية تطبيق النصوص القانونية القائمة على ما أفرزته وسائل الاتصال الحديثة، وتحديدًا شبكات الإنترنت من معاملات إلكترونية.

وضمن هذا التوجّه سارت العديد من التشريعات في أوروبا وأمريكا وشرق آسيا، أمّا عن الاتجاه التشريعي العربي للتعامل مع تحديات الوسائل الإلكترونية في الإثبات فإنّ البناء القانوني للتشريعات العربية في حقلي التعاقد والإثبات لم يكن يعرف الوسائل الإلكترونية.

وقد تم الاعتداد مؤخرًا بتوقيع آخر خصوصًا مع تطوّر وسائل الاتصال وظهور ما يسمّى بالتجارة الإلكترونية التي كانت بحاجة إلى تواقيع تتلاءم مع طبيعتها، وهو ما فرض على المشرع الإماراتي وعلى غرار باقي التشريعات المقارنة النص على هذا التوقيع الذي يصطلح بالتوقيع الإلكتروني من خلال المادة (17) مكرّر إلى القانون الاتحادي رقم 36 لسنة 2006 بتعديل قانون الإثبات رقم 10 لسنة 1992 وصدور القانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية من قِبل صاحب السمو الشيخ خليفة بن زايد آل نهيان، وينطبق القانون على السجلات والمستندات والتوقيعات الإلكترونية ذات العلاقة بالمعاملات والتجارة الإلكترونية، ويستبعد المعاملات والقضايا المتعلّقة بالأحوال الشخصية كالزواج والطلاق والوصايا. كما أنّه لا ينطبق على سندات ملكيّة الأموال غير المنقولة، والسندات القابلة للتداول، والمعاملات المتعلّقة ببيع وشراء الأموال غير المنقولة والتصرّف بها، وأيّ وثائق تتطلّب تصديقها أمام الكاتب العدل وفقًا للقانون.

وتشمل أهداف هذا القانون حماية حقوق المتعاملين إلكترونيًّا وتحديد التزاماتهم، وتشجيع وتسهيل المعاملات والمراسلات الإلكترونية من خلال السجلّات الإلكترونية الموثوق بها، والحدّ من حالات تزوير المراسلات الإلكترونية وإرساء مبادئ موحّدة للّوائح والمعايير المتعلّقة بسلامة المراسلات الإلكترونية.

مشكلة الدراسة:

أدّت ثورة الاتصالات والمعلومات والتطوّر التقنيّ الكبير في استخدام الحاسب الآلي وشبكة الإنترنت إلى تطور كبير في التعاملات والتجارة الإلكترونية وظهور التوقيع الإلكتروني، وهو توقيع يستخدم في العقود الإلكترونية المبرمة عبر شبكة الإنترنت، فأصبحت معظم التعاملات المالية والتجارية تتم بواسطة الكتابة الإلكترونية والمحررات الإلكترونية، ولذلك ظهر بديلاً عن التوقيع الخطي التقليدي توقيع إلكتروني يتوافق مع طبيعة التصرفات القانونية والعقود التي تتم باستخدام وسائل التقنية الحديثة.

ولقد أثار هذا الجيل الجديد من التواقيع جدلاً قانونيًّا بخصوص القبول به والاعتراف بقوّته القانونية في نسبة المستند إلى صاحبه، ذلك أنّ استعمال التقنية العالية في إبرام العقود مكّن من الانتقال من عالم الأوراق والوثائق الورقية إلى عالم البيانات المشفّرة المحمّلة على دعامات غير مادية، ممّا ألزم وجوب تدخل تشريعي لتحيين المقتضيات القانونية المتعلّقة بالتواقيع الخطية، وجعلها مواكبة للتطور العلمي والتكنولوجي الحاصل في ميدان المعلومة وطرق تخزينها وانتقالها، مع إقرار شروط ومعايير معيّنة للأخذ بهذه التواقيع في الإثبات، وبخاصة على مستوى درجات التوثق من مصدرها، وكذا درجات الحماية المقررة لها من عمليات الاعتداء أو التزوير، وتظهر مشكلة الدراسة من خلال الإجابة عن التساؤل الآتي: ما مدى حجية التوقيع الإلكتروني في الإثبات؟

تساؤلات الدراسة:

يحاول الباحث من خلال دراسته الإجابة عن التساؤلات الآتية:

1. ما هو مفهوم التوقيع الإلكتروني؟ وما هي خصائصه؟
2. ما المقصود بتشفير التوقيع الإلكتروني؟ وما هي صوره؟
3. كيف يمكن تصديق التوقيع الإلكتروني؟ وما الجهة المسؤولة عنه؟
4. ما هي شروط حجية التوقيع الإلكتروني؟ وما هي الآثار المترتبة على توافر شروط حجية التوقيع الإلكتروني؟
5. ما أهم التطبيقات المستخدمة في التوقيع الإلكتروني؟
6. ما هي وظيفة التوقيع الإلكتروني في الإثبات؟ وما مدى حجية التوقيع الإلكتروني في الإثبات؟

أهداف الدراسة:

تهدف هذه الدراسة إلى مناقشة موضوع حجية التوقيع الإلكتروني في الإثبات دراسة مقارنة، وإبراز صور التوقيع الإلكتروني وتشفيره وشروط حجيته وآثاره في ظل الجهود الدولية، وبيان أهم التطبيقات المستخدمة في التوقيع الإلكتروني؛ وموقف الأنظمة القانونية المختلفة من حجية التوقيع الإلكتروني في الإثبات.

منهج الدراسة:

اعتمد الباحث في تنفيذ هذه الدراسة التي تتمحور حول حجية التوقيع الإلكتروني في الإثبات المنهج التحليلي والمقارن، حيث عمل الباحث على تحليل ما جاء في القانون الإماراتي بشأن حجية التوقيع الإلكتروني في الإثبات ومقارنته مع التشريعات الأخرى حتى يتسنّى لنا التوصية بشأن ما نراه يصبّ في صالح النظام القانوني الإماراتي من خلال دراسة في التشريع الإماراتي والتشريعات المقارنة.

خطة الدراسة:

سيقوم الباحث في دراسته بتناول مفهوم التوقيع الإلكتروني في المبحث التمهيدي، بحيث سيتطرّق إلى تعريف التوقيع الإلكتروني، ومن ثمّ سيتدرج بالحديث في موضوع خصائص التوقيع الإلكتروني.

كما سيتطرّق في الفصل الأول إلى القوة الفنية والثبوتية للتوقيع الإلكتروني، وذلك من خلال الإشارة إلى آلية تشفير التوقيع الإلكتروني، بالإضافة إلى طرق التحقّق من سلامة الرسالة والمصادقة عليها.

أمّا في الفصل الثاني فستتم مناقشة شروط حجية التوقيع الإلكتروني وآثاره في الإثبات، وذلك من خلال شروط حجيته بالإضافة إلى الآثار المترتّبة على توافر شروط الحجية، كما سيتناول الباحث وظيفة وحجية التوقيع الإلكتروني في الإثبات.

ثم ستنتهي الرسالة بالخاتمة التي ستتضمّن أهم النتائج والتوصيات، حيث ستتوصّل إلى نتائج، والتي يتمنى الباحث أن تثري المكتبة القانونية، كما سيتم اقتراح بعض الاقتراحات على ذوي الشأن والاختصاص سواء على المستوى الوطني أم العربي أم الدولي.

المبحث التمهيدي

ماهية التوقيع الإلكتروني

تمهيد وتقسيم:

أدّى التطور التكنولوجي السريع الذي نعيشه الآن، والذي يطلق عليه عصر ثورة المعلومات والبيانات إلى ظهور وسائل وأساليب جديدة في إبرام عقود لم تكن معروفة منذ سنوات قليلة وهذه الوسائل في تطور دائم ومستمر وسريع، ولمّا كان القانون هو مرآة الواقع كان لا بد للمشرع من إصدار تشريعات لمعالجة ما استجد من وسائل وطرق لإبرام العقود.

وقد حاولت مجموعة من المنظمات الدولية تقديم تعريف للتوقيع الإلكتروني سواء من خلال قوانين مرتبطة بالتجارة الإلكترونية، أم من خلال قوانين خاصة بالتوقيع الإلكتروني، وتعتبر منظمة الاتحاد الأوروبي ومنظمة الأمم المتحدة للتجارة الدولية المعروفة بالأونسيترال، أهمّ المنظمتين اللتين قدّمتا تعريفًا للتوقيع الإلكتروني.

إنّ إصدار المشرع الإماراتي لقانون متعلّق بالتبادل الإلكتروني وتنصيصه على التوقيع الإلكتروني، من قِبل صاحب السمو الشيخ خليفة بن زايد آل نهيان، والذي ينطبق على السجلات والمستندات والتوقيعات الإلكترونية ذات العلاقة بالمعاملات والتجارة الإلكترونية[1]، يجعلنا نتساءل عن المقصود بهذا التوقيع باعتباره مصطلحًا جديدًا، وعلى ضوء ذلك سأتناول ماهية التوقيع الإلكتروني من خلال المباحث الآتية:

---

1 القانون الاتحادي رقم 2006/36 بتعديل قانون الإثبات رقم 10/ 1992 والقانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية.

- **المطلب الأول:** تعريف التوقيع الإلكتروني
- **المطلب الثاني:** خصائص التوقيع الإلكتروني وأهميته

المطلب الأول: تعريف التوقيع الإلكتروني

ذُكرت للتوقيع الإلكتروني تعريفات متعددة، منها ما أورده الفقه في شـــروحاته، ومنها ما جاء في النصوص التشريعية في القوانين المقارنة، ومن التعريفات الفقهيـــة تلك التي حاول أصحابها الجمع بين التعريـــف التقنـــي للتوقيـــع الإلكترونـــي؛ أي: التعريف الذي يرتكز على الوسائل التقنية التي يقوم عليهـــا التوقيـــع الإلكترونـــي، والتعريف الوظيفي؛ أي: التعريف الذي يرتكز على الوظائف التي يقوم بها التوقيع.

الفرع الأول: التعريف التشريعي للتوقيع الإلكتروني

لقد حاولت أغلب الدول العربية مسايرة التطوّرات الحاصلة على مختلف وسائل الاتصال الحديثة، الشيء الذي دعا إلى إصدار ترسانة قانونية جديدة تساير هذه التطورات.

فلقد أضاف المشرع الإماراتي المادة (17) مكرر إلى القانون الاتحـــادي رقـــم 2006/36 بتعديل قانون الإثبات رقم 10/ 1992، حيث نصّت على "يعتبر توقيعًـــا إلكترونيًّا كلّ أحرف أو أرقام أو رموز أو إشارات أو صور أو أصوات لهـــا طـــابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره على النحو الوارد في

قانون المعاملات والتجارة الإلكترونية"[1].

وقد عرف قانون المعاملات والتجارة الإلكترونية لإمارة دبي التوقيع الإلكتروني بأنه[2] "توقيع مكوّن من حروف أو أرقام أو رموز أو صوت أو نظـام معالجـة ذي شكل إلكتروني وملحق أو مرتبط منطقيًّا برسالة إلكترونية وممهور بنيـة توثيـق أو اعتماد تلك الرسالة"[3].

كما عرف قانون المعاملات والتجارة الإلكترونية لإمارة دبي التوقيع الإلكتروني المحمي الذي يتمتّع بحماية القانون بأنه "ذلك التوقيع الذي استوفى الشروط المنصوص عليها في المادة (20) من القانون المذكور"[4].

وعرّف قانون المعاملات والتجارة الإلكترونية لإمارة دبي أداة التوقيع بأنها[5] "جهاز أو معلومات إلكترونية معدّة بشكل فريد لتعمل بشكل مستقلّ أو بالاشتراك مع أجهزة ومعلومات إلكترونية أخرى على وضع توقيع إلكتروني لشخص معيّن، وتشمل هذه العملية أيّة أنظمة أو أجهزة تنتج أو تلتقط معلومات فريدة مثل رموز أو مناهج، وعرف الموقع بأنه الشخص الطبيعي أو المعنوي الحائز لأداة توقيع إلكتروني خاصة به، ويقوم بالتوقيع أو يوقع نيابة عنه على الرسالة الإلكترونية باستخدام هذه الأدلة.

---

1 المادة (17) مكرر من القانون الاتحادي رقم 36/ 2006 .

2 المادة (2) من قانون المعاملات والتجارة الإلكترونية رقم (2) لسنة 2002 لإمارة دبي.

3 أسامة روبي عبد العزيز الروبي، حجية التوقيع الإلكتروني في الإثبات والادعاء مدنيًّا بتزويره وفقًا لقانوني الإثبات والمعاملات الإلكترونية العماني دراسة مقارنة بالقانونين المصري والفرنسي، دار النهضة العربية، 2010م، ص 5.

4 المادة (20) من قانون التجارة الإلكترونية لإمارة دبي لعام 2002م.

5 المادة (20) من قانون المعاملات والتجارة الإلكترونية رقم (2) لسنة 2002 لإمارة دبي.

يتبيّن من خلال تلك التعريفات أنها من أكثر القوانين اتفاقًا مع قانون الاونسيترال النموذجي بشأن التجارة الإلكترونية[1].

وقد عرف المشرع المصري التوقيع الإلكتروني على أنه[2] "ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متفرّد يسمح بتحديد شخص الموقع ويميزه عن غيره. والواضح من هذا التعريف أنه تعريف مختلط حيث يجمع بين التعريف التقني والوظيفي، فهو قد حدّد شكل التوقيع الإلكتروني بأنه يتّخذ شكل حروف أو.. ثم أضاف كلمة (وغيرها) حتى يسمح بدخول أيّ وسيلة جديدة تظهر مع التطور التكنولوجي، ولكنه في شقّه الوظيفي، عندما تعرض للوظائف التي يجب أن يحقّقها التوقيع، لم يتعرّض إلا لوظيفة واحدة وهي تحديد هوية الموقع، دون الإشارة إلى الوظيفة الثانية المتعلّقة برضاء الموقع على ما تمّ التوقيع عليه[3].

وعرف المشرع الأردني التوقيع الإلكتروني بأنه "البيانات التي تتّخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أيّ وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقّعها، ويميّزه عن غيره

---

1 الأستاذ. منير محمد الجنبيهي، الأستاذ. ممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، 2008م، ص83 .

2 القانون رقم (15) لسنة 2004 الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المادة (1/ج).

3 القانون رقم (15) لسنة 2004 في المادة (1/ ج).

من أجل توقيعه وبغرض الموافقة على مضمونه[1].

ويلاحظ من التعريف السابق أن المشرع الأردني عرف التوقيع الإلكتروني بأنه (بيانات) وحاول أن يبين أشكال هذه البيانات، فقد تكون عبارة عن حروف أو أرقام أو رموز.. واشترط المشرع الأردني في هذه البيانات أن تتم بطريقة (شكل) إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة. واشترط أيضًا في هذه البيانات ان تكون مدرجة في رسالة المعلومات وهو ما يعبر عنه بشرط اتصال التوقيع بالسند[2].

وعرف المشرع العماني التوقيع الإلكتروني بأنه[3] "التوقيع على رسالة أو معاملة في شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع وتمييزه عن غيره"[4].

فمن خلال التعريفات السابقة يمكن القول أن التوقيع الإلكتروني يجب أن يكون من حروف وأرقامًا أو رموز أو إشارات وغيرهم وأن يكون مرتبطًا برسالة بيانات أو محرر وأن يكون مميزًا ومحددًا لهوية صاحبه وأن يكون بوسيلة موثوق بها[5].

وبعد هذا العرض نخلص إلى القول بأنّ التشريعات العربية تتشابه في تعريفها

---

1 المادة (2) من قانون المعاملات الإلكترونية.

2 مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الإنترنت، دار الكتب القانونية، مصر، 2010م، ص 154.

3 المادة الأولى من قانون المعاملات الإلكترونية العماني، الصادر بالمرسوم السلطاني رقم (69) لسنة 2008م.

4 أسامة روبي عبد العزيز الروبي، حجية التوقيع الإلكتروني في الإثبات والادعاء مدنيًّا بتزويره وفقًا لقانوني الإثبات والمعاملات الإلكترونية العماني، مرجع سابق، ص 5.

5 أ. أيمن علي حسين، التوقيع الإلكتروني بين النظرية والتطبيق، مرجع سابق، ص 31.

للتوقيع الإلكتروني فقد بينت التقنية الإلكترونية المستخدمة في تكوين التوقيع الإلكتروني، وحددت وظيفة التوقيع الإلكتروني في تحديد هوية الموقع والتعبير عن إرادته في الالتزام بما وقع عليه ويمكننا تعريف التوقيع الإلكتروني بأنه "بيانات معالجة إلكترونيًّا ترتبط بوثيقة إلكترونية من شأنها تحديد هوية الموقع، وتمييزه عن غيره، والتعبير عن إرادته في الالتزام بمضمون هذه الوثيقة"، ويسمح هذا التعريف بقبول التقنيات المختلفة التي تجسّد التوقيع الإلكتروني دون تحديد آليات معيّنة بذاتها، وهذا يتناسب مع التطور التكنولوجي والتقني المتزايد باستمرار الذي يفرض تقنيات جديدة يمكن استخدامها لتكوين التوقيع الإلكتروني ذلك أنّ مواكبة التطوّر التكنولوجي الحاصل تؤدّي إلى ازدهار التجارة الإلكترونية وتطويرها.

وبمطالعة لائحة التوقيع الإلكتروني الصادرة في 2002/3/8م في المملكة المتحدة يتبيّن أنها تضمّنت في الفصل الأول منها تعريفاً للتوقيع الإلكتروني حيث ورد فيها أنه "بيانات في شكل إلكتروني ملحقة أو متحدة منطقيًّا بغيرها من البيانات الإلكترونية والتي تصلح كوسيلة للتوقيع"[1].

أمّا قانون الأونسيترال لعام 1996م فقد عرف التوقيع "إذا اشترط القانون وجود توقيع من شخص يستوفي ذلك إذا استخدمت طريقة لتعيين هوية الشخص والتدليل على موافقته للمعلومات الواردة في رسالة البيانات"[2].

كما جاء في قانون الأونسيترال لعام2001م تعريف التوقيع الإلكتروني بأنه

---

1 المستشار الدكتور محمد الشهاوي، شرح قانون التوقيع الإلكتروني رقم (15) لسنة 2004 دراسة مقارنة، الطبعة الأولى، 2010م، ص 24.

2 انظر المادة 7/ 1/ أ من قانون الأونسيترال لعام 1996.

"البيانات الإلكترونية الموجودة في رسالة البيانات المرتبطة بها منطقيًّا، والتي تستخدم للتحقّق من شخصية الموقّع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[1].

والظاهر من هذا التعريف أنه يلحظ الجانب الوظيفي، حيث لم يذكر أيّ صورة من صور التوقيع الإلكتروني، إنما ذكر وظائف التوقيع وإنها الفيصل في تحديد ما إذا كانت وسيلة معينة يمكن اعتبارها توقيعًا إلكترونيًّا أم لا.

وقد أقرّت اللجنة الأوروبية في 13 ديسمبر 1999م قرارًا يتعلّق بالتوقيع الإلكتروني ميّزت فيه بين التوقيع البسيط وهو الذي يتمّ إنشاؤه متّصلاً أو مرتبطًا ببرمجيات الآخرين وبطريقة معتمدة، والتوقيع الإلكتروني المتقدّم، وهو الذي يتطلّب أن يكون مرتبطًا بالموقع مجرّدًا، وأن يسمح بإثبات شخصية الموقع ويكون منشأ بوسائل الموقع وتحت رقابته الخاصة، ويكون مرتبطًا بمصدره بحيث يمكن معرفة كلّ تعديل لاحق[2].

وقد عرف القانون المدني الفرنسي في المادة (1316/ 4) في الفقرة الثانية التوقيع تحت الشكل الإلكتروني أنه: يجب أن يتمّ باستخدام إجراء مضمون لإثبات شخصية صاحبه وضمان ارتباطه بالعمل المقصود[3].

---

1 انظر: المادة 2/ أ من قانون الأونسيترال 2001 الخاص بالقانون النموذجي للتوقيعات الإلكترونية.

2 انظر: طاهر شوقي مؤمن، عقد البيع الإلكتروني، بحث في التجارة الإلكترونية، دار النهضة العربية، القاهرة، 2007م، ص 72.

3 Piette – coudel – la signature electonique –ed litec 2001 –n 4 p2 . أشار إليه طاهر شوقي، مرجع سابق، ص 73.

وقد عرّف القانون المدني في لوكسمبورغ التوقيع الإلكتروني على أنه: كلّ علامة صادرة من شخص تدلّ على اسمه أو على أيّ خاصية من خصائصه تعبر عن رضاه بالتعاقد[1].

الفرع الثاني: التعريف الفقهي للتوقيع الإلكتروني

يعرف بعض فقهاء القانون التوقيع الإلكتروني بأنه "إجراء معيّن يقوم به الشخص المراد توقيعه على المحرّر بغضّ النظر عن شكله سواء أكان رقمًا أم شفرة معيّنة، ممّا يحفظ السرية ويعطي الثقة في دلالة التوقيع على صاحبه"[2].

ويعرّفه البعض بأنه "طريقة اتصال مشفّرة تعمل على توثيق المعاملات التي تمّت بواسطة شبكة الإنترنت، وأن الفكرة والهدف والنية الأساسية للتوقيع هي نفسها في التوقيع اليدوي مع اختلاف الأداة والكيفية وأسلوب التوقيع"[3].

ويعاب على هذا التعريف والذي سبقه أنّهما قد ذكرا بعض صور التوقيع الإلكتروني دون الصور الأخرى، كما أنّهما لم يذكرا وظائف التوقيع الإلكتروني واقتصرا على ذكر وظيفة واحدة فقط، وهي وظيفة تعيين هوية الموقع، ولم يتعرّضا للوظيفة الأخرى للتوقيع، وهي الخاصة برضاء الموقع بمضمون المحرر.

---

1 إيمان مأمون أحمد، الجوانب القانونية لعقد التجارة الإلكترونية، القاهرة، دار النهضة العربية، 2005م، ص 252.

2 سامح عبد الواحد التهامي، التعاقد عبر الإنترنت، مصر، دار الكتب القانونية، 2008م، ص 380 .

3 محمد خالد جمال رستم، التنظيم القانوني للتجارة والإثبات الإلكتروني في العالم، منشورات الحلبي الحقوقية، بيروت، 2006م، ص 39.

وكذلك يعرف على أنه "عبارة عن القيام بعمل أو إجراء يقوم به المرسل بحيث يتم ربط هويته بالوثيقة ليتسنّى للمستلم التحقّق من صحة التوقيع"[1].

فهناك فرق بين التوقيع الإلكتروني والإمضاء المعروف الذي يتم غالبًا على الورق، بل أنه نص قصير يضاف إلى بداية الوثيقة أو نهايتها، وقد يكون منفصلاً عنها تمامًا، كأن يرسل في ملف خاصّ مستقل[2].

ويعرفه آخر بأنه "بيان مكتوب في شكل إلكتروني يتمثّل في حرف أو رقم أو رمز أو إشارة أو صوت أو شفرة خاصة ومميزة ينتج من اتّباع وسيلة آمنة، وهذا البيان يلحق أو يرتبط منطقيًا ببيانات المحرّر الإلكتروني للدلالة على هوية الموقع على المحرر والرضاء بمضمونه"[3].

من هذا التعريف يتبين أن التوقيع الإلكتروني حتى ينشأ صحيحًا منتجًا آثاره القانونية، لا بد أن يعبّر عن هوية الموقع، كما يجب أن يكون هذا التوقيع قد صدر صحيحًا من الموقع، وهذا أمر لا يتأتى إلا بسيطرة الموقع على عناصر التوقيع.

وعليه فإنّني أميل إلى التعريف الذي يركز على الجانب الوظيفي، دون الجانب التقني، فالتعريف الوظيفي يقوم على أساس وظائف التوقيع وهي ثابتة، على عكس التعريف التقني الذي يعاب عليه أنه لا يمكن من خلاله حصر صور التوقيع التي

---

1 آزاد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2015م، ص 35 .

2 محمد حسن قاسم، أصول الإثبات في المواد المدنية والتجارية، منشورات الحلبي الحقوقية، بيروت، لبنان، بدون سنة طبع، ص 160.

3 عبد العزيز المرسي حمود، مدى حجية المحرر الإلكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافذة، بحث منشور في مجلة البحوث القانونية والاقتصادية، كلية الحقوق بجامعة القاهرة، العدد 11، السنة 11، أبريل، 2002م، ص 39.

تكون قابلة للتطور، لذلك نتّفق مع من يذهب إلى تعريف التوقيع الإلكتروني على أنه (مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنــه هــذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته)[1].

المطلب الثاني: خصائص التوقيع الإلكتروني وأهميته وصوره

يعدّ التوقيع من المبادئ الأساسية في الإثبات وشرطًا مهمًّا لتوثيق أيّ مستند سواء في المراسلات العادية أم الإلكترونية على اختلاف أنواعها ووسائطها في داخل المؤسسة أو المراسلات التي تتم بين المؤسسات في داخل الدولة أو خارجها، وهذا بدوره يتماشى مع مقتضيات التجارة الإلكترونية، وفيه استجابة وتيسير لمعاملات التجار الذين يرغبون في إقامة علاقات تعاقدية عبر الإنترنت، ومن هنا تكمن مقاصد المشرع من حيث أهمية التوقيع الإلكتروني في مدى السرية، والضمان الذي يتمتّع به، وأيضًا خصائصه التي يتميّز بها عن التوقيع العادي.

الفرع الأول: خصائص التوقيع الإلكتروني

يتميز التوقيع الإلكتروني بعدة خصائص أهمّها ما يأتي:

1. التوقيع الإلكتروني يتم عبر وسائل إلكترونية وعن طريق أجهزة الحاسب الآلي والإنترنت أو أسطوانة[2]، حيث أصبح بإمكان أطراف العقد الاتصال ببعضهم

---

1 محمود ثابت محمود، حجية التوقيع الإلكتروني في الإثبات، مجلة المحاماة، العدد الثاني، 2002م، ص 20.

2 عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، ط الأولى 2010م، ص 149.

البعض والاطلاع على وثائق العقد والتفاوض بشأن شروطه وكيفية إبرامه وإفراغه في محرّرات إلكترونية، وأخيرًا إجراء التوقيع الإلكتروني عليه[1].

على خلاف التوقيع التقليدي الذي يوضع على دعامة مادية هي في الغالب دعامة ورقية، في هذه الحالة تذيل الكتابة بالتوقيع فتحول الدعامة بعد ذلك إلى مستند صالح الإثبات.

2. لم يشترط في التوقيع الإلكتروني صورة معينة حيث إنه يمكن أن يأتي على شكل حرف أو رمز أو رقم أو إشارة أو حتى صوت، المهم فيه أن يكون ذا طابع منفرد يسمح بتمييز شخص صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه[2].

بخلاف التوقيع التقليدي الذي يقتصر على الإمضاء بخط اليد، وقد يضاف إليه الختم وبصمة الأصابع[3].

3. التوقيع الإلكتروني يعدّ علمًا وليس فنًّا، وبالتالي يصعب تزويره، أمّا التوقيع التقليدي فهو عبارة عن رسم يقوم به الشخص؛ أي: أنه فنّ وليس علم، وبالتالي فإنه يسهل تزويره أو تقليده[4]، حيث إنّ الوظيفة الرئيسية للتوقيع الإلكتروني هي

---

1 بشار محمود دودين، الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، دار الثقافة للنشر والتوزيع، ط 2، 2010م، ص 247.

2 عباس العبودي، مرجع سابق، ص 149.

3 عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة لنشر والتوزيع، الطبعة الأولى، 2009، الصفة: 32 وما بعدها.

4 نور الدين الناصري، المعاملات الإلكترونية في ضوء القانون رقم (53/05) المتعلّق بالتبادل الإلكتروني للمعطيات، مجلة القانون الإقتصادي العدد الثاني، يناير 2009م، مطبوعات الهلال، وجدة، المغرب، ص 139.

الاستيثاق من مضمون المحرر الإلكتروني وتأمينه من التعديل بالإضافة أو الحذف، وذلك عن طريق ربط المحرر الإلكتروني والتوقيع الإلكتروني بحيث يقتضي إجراء أيّ تعديل لاحق إيقاع توقيع إلكتروني جديد. كما أنّ التوقيع بالشكل الإلكتروني يقوم أيضًا بمنح المستند الإلكتروني صفة المحرّر الإلكتروني، وبالتالي يجعل منه دليلاً معدًّا مسبقًا للإثبات له منزلة الدليل الكتابي نفسه الذي يتم إعداده مسبقًا قبل أن يثور النزاع بين الأطراف[1].

4. إنّ التوقيع الإلكتروني، وعلى العكس من التوقيع الكتابي لا يقتصر على الإمضاء أو بصمة الأصابع بل يشمل صورًا لا يمكن حصرها، منها الحروف والأرقام والصور والرموز والإشارات وحتى الأصوات، كلّ ذلك بشرط أن يكون لها طابع فردي، يسمح بتمييز الشخص صاحب التوقيع وتحديد هويّته، وإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه، فالتوقيع الإلكتروني على رسالة ما أو وثيقة هو عبارة عن بيانات متجزئة من الرسالة ذاتها (جزء صغير من البيانات) يجرى تشفيره[2] وإرساله مع الرسالة، بحيث يتم التوثّق من

1 بشار محمود دودين، مرجع سابق، ص 248 .

2 ويرتبط التوقيع الإلكتروني بالتشفير ارتباطًا عضويًّا، فالتشفير هو عملية لتغيير البيانات بحيث لا يمكن قراءتها إلا من قبل الشخص المستخدم وحده باستخدام مفتاح فك التشفير، والطريقة الشائعة للتشفير تتمثّل في وجود مفتاحين، المفتاح العام وهو معروف للعامة، والمفتاح الخاص الذي يتوفر فقط لدى الشخص الذي أنشأه، ويمكن بهذه الطريقة لأيّ شخص يملك المفتاح العام أن يرسل الرسالة المشفرة، ولكن لا يستطيع أن يفك شفرتها إلا الشخص الذي لديه المفتاح الخاص، ويجب في هذا الصدد عدم الخلط بين التوقيع الإلكتروني وبين تشفير الرسالة الإلكترونية، فصحيح أن كليهما يقوم على عملية حسابية يتم من خلالها تشفير مضمون التوقيع أو الرسالة، ولكن هناك فرق وهو أن تشفير الرسالة يشملها بأكملها، في حين أن التشفير في التوقيع

صحة صدور الرسالة من الشخص عند فكّ التشفير، وانطباق محتوى التوقيع على الرسالة.

5. إنّ التوقيع الإلكتروني يتميّز بأنه لا يتم عبر وسيط مادي؛ أي: دعامة ورقية، بحيث تذيل به الكتابة، كما هو الحال بالنسبة للتوقيع الكتابي، وإنما يتم كلّيًّا أو جزئيًّا عبر وسيط إلكتروني من خلال أجهزة الكمبيوتر، أو عبر الإنترنت، بحيث يكون بإمكان أطراف العقد الاتصال ببعضهم البعض والاطلاع على وثائق العقد، والتفاوض بشأن شروطه وإفراغ هذا العقد في محرّرات إلكترونية، وأخيرًا التوقيع عليها إلكترونيًّا[1].

6. لزوم تدخل طرف ثالث يقوم بدور الوسيط بين أطراف العقد، حيث استلزمت ضرورة الأمن القانوني وجوب استخدام تقنية آمنة في التوقيع الإلكتروني تسمح بالتعرّف على شخصية الموقع[2].

وكما أنّ هناك مزايا للتوقيع الإلكتروني الرقمي أو الكودي، فإنّ له أوجه سلبية تنتقص من هذه المزايا، ومنها:

أوّلاً: احتمال تعرّض الرقم السري –الكودي– للسرقة أو الضياع

وتبقى هذه أكبر السلبيات التي تعاب على التوقيع الرقمي، إلا أنّ هذا القول يبقى مردودًا بأنّ التوقيع التقليدي كذلك معرّض لأخطار التزوير والتقليد، وسرية الرقم

الإلكتروني يقتصر فقط على التوقيع دون بقية الرسالة، بحيث إنه يمكن أن يكون مرتبطًا برسالة غير مشفرة. فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة للنشر، مصر، 2002م، ص 82 و83.

1 أ. محمد بودالي، التوقيع الإلكتروني، مجلة الإدارة، العدد رقم 2، لسنة 2003م، ص 57.

2 راجع بأكثر تفصيل: أ. محمد بودالي، مرجع سابق، ص 57.

تكفي للدلالة على صدوره عن صاحبه الذي يملك التوقيع به، سواء عن قصد أم إهمال، وذلك بحسب الأصل. والعميل على سبيل المثال ملتزم بسرية رقم البطاقة حسب اتفاقه مع البنك وإلا تعرّض للمساءلة القانونية إن ثبت إساءته استخدام هذا الرقم، فضلاً عن ذلك لو كان توقيعه الإلكتروني الصادر به شهادة موثقة من الجهة المختصة، قد تسرّب إلى آخرين فهو مسؤول عن ذلك، طالما أنه لم يتخذ إجراءات الحيطة المنصوص عليها، ولأنه سيكون الوحيد الذي سرب هذا الرقم للغير[1].

وليس هناك إمكانية لاستخدام البطاقة الممغنطة دون استخدام الرقم السري، حيث يعدّ الرقم السري هي مفتاح التشفير المطلوب من الطرف الثاني، ويعدّ توقيعًا إلكترونيًّا مثبتًا لإتمام العملية التي تتم عن طريق البطاقة.

ثانيًا: احتمال تقليد الشريط الممغنط الموجود على البطاقة الائتمانية

وذلك أمر وارد، لكن لا يملك الشخص استعمال البطاقة دون رقمها السري، والرقم السرّيّ لا يعلمه سوى العميل، ونظام الحاسب الآلي الذي أخرج هذا الرقم، حتى مشغل هذا الحاسب الآلي نفسه لدى البنك مصدر البطاقة، لا يستطيع الوصول إلى ذلك الرقم، ولهذا فإنّ تقليد البطاقة ذاتها لا يجدي ما لم يكن الشخص قادرًا على معرفة الرقم السري الذي يمكن عن طريقه استعمال هذه البطاقة[2].

ثالثًا: التوقيع الرقمي لا يعبّر عن شخصية صاحبه مثل التوقيع التقليدي بالكتابة

---

1 جميل عبد الباقي، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية. دار النهضة، القاهرة، 2003م، ص172.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، المحلة الكبري، مصر: دار الكتب القانونية: دار شتات للنشر، 2007م، ص 242 .

لكن ذلك مردود عليه بأنّ التوقيع الإلكتروني لا يصدر عن الحاسب الآلي، وإنما عن صاحب التوقيع وأن الحاسب الآلي وسيلة فقط في أداء هذا التوقيع، تمامًا كما أن القلم وسيلة للتوقيع التقليدي، فعند السحب ببطاقة الائتمان –على سبيل المثال– ومن خلال اتّباع إجراءات معيّنة متّفق عليها بين البنك والعميل بإدخال رقمه السري، وهو بذلك يكون قد وقع ويتم تنفيذ توقيعه عن طريق الحاسب الآلي، وبالتالي فهذا الحاسب الآلي لا إرادة له في تمام هذا التوقيع، لأنّ التوقيع منسوب للشخص وليس للآلة، وهي جهاز الحاسب الآلي.

ولذلك نجد أنّ العميل ملزم بالمحافظة على رقمه السري للبطاقة، والإبقاء عليه في الكتمان، وذلك لأنه بمثابة مفتاح خزانة النقود ما دام أنه يمكّن من دخول الحساب المصرفي للعميل لدى البنك الذي أصدر البطاقة، ومن إجراء أية عملية تحويل أو خصم أو سحب، لذلك غالبًا ما يوصي البنك باتخاذ بعض الاحتياطات والتحلي بالحيطة والحذر عند أيّ استعمال للرقم السري للبطاقة، لذلك يستحسن عدم وضع الرقم السري مع البطاقة أو كتابته على أية دعامة ورقية.

إنّ التزام صاحب البطاقة بالإخطار عن فقدها أو سرقتها هي ورقمها السري في آن واحد هو التزام أساسي، وذلك لأنّ استخدام أجهزة التوزيع الآلي للنقود (D.A.B) يتطلب معرفة الرقم السري، لذلك فإنّ البنك المصدر الذي لم يتم إخطاره بواقعة الفقد أو السرقة للرقم السري مع البطاقة لا يمكنه محو برمجة الأجهزة في الحال، بحيث تمتنع عن قبول بطاقة السحب مستقبلاً، أو أن تقوم بإلغائها، ويترتّب على ذلك أن حامل البطاقة الذي لم يقم بإخطار البنك بواقعة فقد الرقم السري يرتكب خطأ ويتحمل تبعًا لذلك عمليات السحب غير المشروعة التي تمت باستخدام البطاقة المسروقة أو

المفقودة رغم معارضته التي جاءت مستترة، فقيام سارق البطاقة الذي عثر عليها باستخدامها في السحب يعدّ قرينة على إهمال الحامل في الإبقاء على الرقم السري طي الكتمان[1].

ولهذا السبب يسأل صاحب الرقم السري عن خطئه أو إهماله في الحفاظ على رقمه السري، ويتحمل المسؤولية المدنية عن العمليات المنفذة قبل إخطاره، والفواتير الخاصة بها ولو وردت بعد الإخطار بواقعة السرقة، ولذلك فإنّه يعفى حامل البطاقة من المسؤولية عن الاستعمال غير المشروع للبطاقة بواسطة الغير من لحظة إخطاره للبنك المصدر بخطاب مسجل أو تلغراف أو بإخطار مكتوب مسلم للبنك، فحامل البطاقة الزرقاء الذي لم يتخذ الحيطة والحذر المنصوص عليهما في الاتفاق المبرم بينه وبين البنك المصدر للبطاقة لا يعفى من المسؤولية عن العمليات المنفذة لدى التجار الذين قاموا بتسليم سلع بناءً على الصكّ المسروق لا سيما أن الحامل الذي ترك البطاقة داخل سيارته الموضوعة في الشارع يعدّ إهمالاً واضحًا[2].

وعليه فإنّ مسؤولية صاحب التوقيع الرقمي، لا تنتفي إلا ابتداء من التاريخ الذي يقوم فيه بالإبلاغ عن حالة السرقة أو الفقدان. وذلك بالنسبة لجميع العمليات التي تنفد بعد الإخطار، حيث يلتزم البنك بنشر معارضة الزبون عقب الفقد أو السرقة مع الرقم السري؛ أي: "التوقيع الرقمي". سيما أن البنك ملزم بفحص التوقيعات الموجودة على الفواتير، متى صدرت هذه الفواتير بعد معارضة الحامل الشرعي للبطاقة، ولا

---

1 جميل عبد الباقي، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، مرجع سابق، ص177.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 244.

يجوز للبنك أن يدفع المسؤولية عن نفسه بأنه في وضع لا يمكنه من عمل هذه الرقابة[1].

وهذا التوقيع الرقمي أو الكودي، مثل سائر البيانات المعلوماتية يمكن تشفيره حفاظاً على سريته. والتشفير إجراء –كما سنرى لاحقًا– يؤدّي إلى توفير الثقة في المعاملات الإلكترونية وذلك باستخدام أدوات أو أساليب لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها غير المشروع.

ويسمح نظام التشفير بتلافي بعض المخاطر المتوقّعة من استخدام الطرق الإلكترونية في المعاملات التجارية، حيث يتم التأكّد عن طريقه من أنّ المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها، بحيث يتأكد المرسل إليه الذي يستطيع عن طريق استخدام وسائل فنية الاطلاع على محتوى المعلومة[2].

ولقد جرم قانون التجارة الإلكترونية الإماراتي تزويــر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة نشاط من الهيئة من خلال إنشاء شهادة تتضمن بيانات غير صحيحة مع العلم بذلك أو نشرها أو تقديمها، لأي غرض غير مشروع،

1 لهذا قضت محكمة باريس بالتزام البنك بالرقابة على التوقيعات المحفوظة لديها في دعوى تعرض فيها أحد العملاء لدى البنك لحادث سرقة شملت حافظة أوراقه التي تحتوي على بطاقته الشخصية ودفتر الشيكات ورخصة القيادة وبطاقته الائتمانية– مشار إليه لدى جميل عبد الباقي، مرجع سابق، ص183 وما بعدها.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 245.

وقد ورد النص على هذه الجريمة في المادة (29) من هذا القانون حماية للتوقيع الإلكتروني.

ويتحقّق فعل الإنشاء باختلاق الشهادة التي لا وجود لها، أمّا النشر فيكون بإنشاء شهادات غير صحيحة ثم استعمالها، والصورة الثالثة تتمثّل في الحصول على شهادة منشأة لدى الغير، ثم مدّ الآخرين بها للاستعمال أو يستعملها الجاني لنفسه[1].

وفي كلّ هذه الصور يكون الغرض غير مشروع أو احتيالي، حيث يتم التسليم بصحة بيانات التوقيع الإلكتروني، كما جرم المشرع الإماراتي فعل تقديم بيانات مزورة لمزود خدمات التصديق، وذلك في المادة (30) من القانون السابق الذكر.

وهنا نرى "أن هذه الجريمة تقترب إلى حدّ ما من التزوير التقليدي، فقد ينتحل الجاني هوية غيره أو يبدل شخصيته، لإنشاء شهادة تصديق إلكتروني غير صحيحة[2].

الفرع الثاني: أهمية التوقيع الإلكتروني وصوره

أوّلاً: أهمية التوقيع الإلكتروني

يمكن الاستفادة من استخدامات التوقيع الإلكتروني في توفير عامل الوقت والجهد الثمين للمواطن والموظف، وفي هذه الحالة لن يضطر المواطن إلى أن يذهب بسيارته أو باستخدام وسائل النقل الأخرى إلى الدوائر الحكومية والانتظار طويلاً كما هو الحال في معظم الدول النامية، بخلاف الدول المتقدمة، حيث إنه بالكاد أن ترى

---

1 عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، 2005م، ص 320 .

2 عبد الفتاح بيومي حجازي، نفس المرجع السابق، ص 323.

أشخاصًا يتابعون وينهون معاملاتهم إلا بأضيق الحالات، وهو ظهور الشخص إن لزم في مسألة شخصية، وبذلك نرى أنّ التوقيع الإلكتروني يسمح بعقد الصفقات عن بعد ودون حضور المتعاقدين.

كذلك يمكن الاعتماد عليه كلّيًا ضمن الإجراءات القانونية والقضائية في المنازعات بين الأشخاص والشركات الخاصة أو المؤسسات والهيئات الحكومية، وهنا يكون لقناعة القاضي دور كبير حيث يتم التعويل على الثقة في الجهاز الذي من خلاله تم إجراء التوقيع الإلكتروني، ويقيم هذه الإجراءات ومدى قوة إجراءات السرية والتخزين والإرسال والحفظ وغيرها، وكفاءة القائمين على هذه الإجراءات، ومدى تقدم التكنولوجيا، كل هذه الاعتبارات ينظرها ويحكم في ضوئها مدى جدارة التوقيع الإلكتروني في أن يتم الاعتماد عليه من عدمه[1].

ويساهم التوقيع في فتح قناة اتصال جديدة بين المواطن والجهات الحكومية يمكن من خلالها النفاذ إلى مستويات الإدارة العليا لزيادة الشفافية في الأعمال الحكومية، وبالتالي يعدّ عاملًا وأداة مهمة لنجاح فكرة الحكومة الإلكترونية.

إنّ التوسّع في استخدام التوقيع الإلكتروني يرفع كفاءة العمل الإداري ويساعد على الإرتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع متطلبات ومستجدات العصر الحديث[2]. وبالتالي يؤدّي هذا النمط إلى التخفيف من نمط البيروقراطية التي تؤخر زيادة النشاطات والمعاملات بكافة صورها، وبما أنّ التوقيع الإلكتروني يتم

---

1 رائد عبد الحميد، مجلة العدالة والقانون، مدى حجية وسائل الاتصال الحديثة في قانون البيانات، رام الله، العدد (2)، لسنة 2005م، ص408.

2 إيناس الخالدي، حجية التوقيع الإلكتروني في الإثبات دراسة في نظام التعاملات الإلكترونية السعودي، كلية الدراسات القضائية والأنظمة، جامعة أم القرى، ص 18.

استخدامه في جميع المستندات ونماذج الطلبات، فإنّ ذلك يساعد على توفير الهوية الرقمية لكلّ مواطن، وهذا يسهم في خلق وعي فكري للمواطن، وتطوير التعامل بالإنترنت، ممّا يؤثّر على التجارة الإلكترونية، فنرى الكثير من الأشخاص الأذكياء الذين يملكون شركات ضخمة حققت الكثير من الأرباح من دون أن يكون لها مقر بحجم الشركات الكبيرة، ومن هنا تكمن أهمية التوقيع الرقمي في أنه يوفر الضمان من خلال استخدام عمليات البيع والشراء من المعاملات الإلكترونية المختلفة كالبيع وغيرها من العقود والتصرفات القانونية التجارية الأخرى والاستيراد والتصدير وباقي التعاقدات، وحجز تذاكر السفر والفنادق والمعاملات المصرفية بكل أنواعها، والتي تتم في شكل محرر إلكتروني موقع توقيعًا إلكترونيًّا، وغير ذلك من المزايا الأخرى التي تؤدي بدورها إلى التوفير في جميع إجراءات إرسال البيانات إلى المواطن والحصول على معلومات منه التوفير في الورق، الطلبات، الطباعة ...إلخ[1].

إنّ التوقيع وضع من أجل تحديد هوية شخص الموقع حيث يعتبر ذلك دليلاً على مشاركة ذلك الشخص بعينه في عملية التوقيع، والربط بين ذلك الشخص ومضمون المستند، ولهذا، فإنّ التوقيع يمكن أن يؤدّي مجموعة متنوّعة من الوظائف حسب طبيعة المستند الذي يحمل التوقيع، فعلى سبيل المثال يمكن أن يكون التوقيع شاهدًا على نيّة الطرف الالتزام بمضمون العقد الموقع عليه، وعلى نية الشخص الإقرار بتحرير النص، أو على نيته تأييد مضمون مستند كتبه شخص آخر، وبذلك يتّضح له مدى الإدراك في ترتّب النتائج القانونية على عملية التوقيع هذه، والتوقيع الإلكتروني

1 إيناس الخالدي، مرجع سابق، ص 18.

قادر على تحديد هوية الشخص الموقع، وبخاصة إذا دعم هذا التوقيع بوسائل توفّر الثقة الكافية، فالتوقيع بالرقم السري قادر على تحديد هوية الشخص الموقع، لأنّ الرقم السري لا يعرفه إلا صاحبه، بحيث لا يستطيع أن ينكر الموقع استخدامه للبطاقة المقترنة برقمه السري "الفيزا" الذي لا يشابه رقمًا آخر ولا يعرفه إلا هو، وكذلك التوقيع بالخصائص الذاتية يحدّد هوية الشخص الموقع لأنّ هذه الخصائص تميزه عن غيره[1]، والحال كذلك في التوقيع الرقمي، والذي سنتطرق إليه لاحقًا وهو شكل من أشكال التوقيع حيث يتم عن طريق المفتاحين العام والخاص بحيث يمكن تحديد هوية الشخص الموقع من خلال قيامه بعملية التشفير المزدوج، إضافة لذلك فإنّ استعانة أطراف العلاقة بجهات التصديق لإصدار شهادات التوقيع المصدق، تؤدّي إلى تحقيق وظيفة التوقيع بتحديد هوية الشخص الموقع، والذي يستخدم هذه الشهادة، وذلك باحتوائها على معلومات هامة عن صاحبها، وبالتالي نجد أن التوقيع الإلكتروني بصوره المتعددة قادر على تحديد هوية الشخص الموقع إذا كان يتمتع بقدر كبير من الثقة في إجراءات توثيقه واستخدامه في تحديد هوية الموقع[2].

كذلك فإنّ التوقيع يعبر عن إرادة الموقع بالموافقة على مضمون السند بوصفة أداة صحة، فهو يعبر عن إرادة صاحبه بالموافقة على ما ورد في السند، وبالتالي فإنّ الموقع عندما يقوم بالتوقيع على المحرر الإلكتروني فإنّ ذلك يعني قبوله والتزامه بما ورد في السند الإلكتروني. وبالتالي، عندما يقوم الموقع بإدخال رقمه

---

1 حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية لنشر، القاهرة، سنة 2002م، ص 45.

2 لورنس محمد عبيدات، إثبات المحرر الإلكتروني، الطبعة الأولى، عمان: دار الثقافة للنشر والتوزيع، 2005م، ص 152 .

السري أو المفتاح الخاص، أو البصمة الجينية على الشاشة فإنّ معنى ذلك هو قبول الشخص لما ورد في هذا المحرر والتزامه به[1]، إذن، وحتى يكون التوقيع صحيحًا يجب أن يكون معبّرًا عن موافقة صاحبه على مضمون ما جاء به من التزامات، وهذا ما أكّده قانون المعاملات الإلكتروني الأردني، حيث نصّت المادة (10/ ب) على أنه " يتم إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه إذا توافرت طريقة لتحديد هويته والدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الذي يحمل توقيعه إذا كانت تلك الطريقة ممّا يعول عليها لهذه الغاية في ضوء الظروف المتعلقة بالمعاملة، بما في ذلك اتفاق الأطراف على استخدام تلك الطريقة "

.ولهذا نرى أن هذا النص يشير إلى استيفاء شرط التوقيع على المحرر في استخدام التوقيع الإلكتروني، فهو بذلك يحقق أهداف التوقيع التقليدي من حيث الدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الموقع إلكترونيًّا، ونص هذه المادة جوهري من حيث إنها إشارات إلى الاعتراف القانوني بالتوقيع الإلكتروني على السجلات والرسائل الإلكترونية كبديل للتوقيع الخطي على السجلات والرسائل المكتوبة تقليديًّا[2].

ثانيًا: صور التوقيع الإلكتروني

---

1 يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات وفقا لقانوني الإثبات والمعاملات الإلكترونية الأردنيين، رسالة ماجستير غير منشورة، الجامعة الأردنية، عمان، الأردن، 2005م، ص 6.

2 لورنس محمد عبيدات، مرجع سابق، ص 153 ، وما بعدها.

نظرًا لما أفرزه التطور التقني في مجالات الاتصالات الإلكترونية، وما أسفر عنه التطور التكنولوجي في مجال نظم المعلومات، فقد ظهرت صور عديدة للتوقيع الإلكتروني بهدف تلافي أيّ قصور في أنظمة تأمين استخدامات شبكة الإنترنت، والعمل على منع عمليات الاحتيال الإلكتروني، وتختلف صور التوقيعات الإلكترونية فيما بينها من حيث درجة الثقة، ومستوى ما تقدّمه من ضمان بحسب الإجراءات المتّبعة في إصدارها وتأمينها والتقنيات التي تنتجها، وتعتبر أهم صور التوقيع الإلكتروني المعروفة وأكثرها انتشارًا حتى الآن، هي التوقيع بالخط الرقمي، والتوقيع بالخواص الذاتية "البيومتري" والتوقيع الرقمي، وهي على التفصيل الآتي:

1. التوقيع الخطي الرقمي:

تتمثّل هذه الصور في نقل التوقيع الخطي إلى الحاسوب عن طريق التصوير بالماسح الضوئي Scanner أو باستخدام القلم الإلكتروني Pen –op وتخزينه على دعامة إلكترونية، فمثلاً عن طريق الماسح الضوئي يتم نقل التوقيع الخطي إلى الحاسوب. حيث تتحوّل العلاقة الخطية إلى صورة تحفظ في شكل ملف، وهو ما يعني أنّ ذلك التوقيع يظهر على جهاز الحاسوب في شكل صورة إلكترونية للتوقيع الخطي، ثم يمكن للشخص أن ينقل هذه الصورة إلى الملف أو الرسالة المراد إضافة التوقيع إليها عبر الإنترنت، كما يمكن تخزينها على أيّ دعامة إلكترونية أو

مغناطيسية محمولة مثل الأقراص المرنة أو المدمجة، علـــى نحـــو يتـــيح للموقـــع استخدامه في التوقيت الذي يختاره في التوقيع على أيّ عقد أو محرر إلكتروني[1].

ويرى جانب من الفقه أنّ هذا التوقيع لا يحقّق المصداقية الكافيـــة مـــن الناحيـــة القانونية، لأنه لا توجد تقنية تؤدّي إلى ربط التوقيع بالمحرر الإلكتروني "الرســـالة"، وبالتالي يستطيع المرسل إليه الاحتفاظ بنسخة من التوقيع التـــي كانـــت علـــى أحـــد المحررات التي وصلت إليه، ثم يعيد وضعها على أي محرر إلكتروني آخـــر، ثـــم يدعي أن التوقيع نقل ووضع على هذا المحـــرر الأخيـــر، وأرســـل عبـــر شـــبكة الاتصالات المفتوحة "الإنترنت" بواسطة صاحب التوقيع الفعلي، ومـــع ذلـــك يـــرى البعض أنه بالإمكان تفادي هذا النقد عن طريق استخدام نظام المفتاح العـــام، الـــذي يستخدم في عمليّتي التشفير وفكّ التشفير لإرسال التوقيع عن طريق شبكة الإنترنـــت إلى أحد الأطراف، واستلامه من قبل الطرف الآخـــر بطريقـــة ســـرية ومأمونـــة، بالإضافة إلى إيجاد جهة تصديق معتمدة يمكن الرجوع إليهـــا للتحقّـــق مقـــدّمًا مـــن شخصية منشئ التوقيع قبل الدخول معه في التعامل[2].

---

1 خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني، دار الجامعة العربية، القاهرة، 2007م، ص 58، تامر محمد عبد الباقي الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت، دراسة مقارنة، منشأة المعارف، 2009م، ص 344، 345.

2 خالد ممدوح إبراهيم، أبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية عام 2006م، ص 200.

كما يمكن استخدام القلم الإلكتروني في نقل التوقيع الخطي إلى الحاسوب، ويتطلب هذا التوقيع استخدام قلم إلكتروني حساس[1]، يمكنه الكتابة على جهاز الحاسوب المعدّ لهذا الغرض، وذلك عن طريق قيام الموقع بوضع توقيعه يدويًا من خلال استخدام القلم الإلكتروني على شاشة الجهاز، ويخزن كمجموعة من القيم الرقمية التي يمكن أن تضاف إلى رسالة البيانات.

ولكن لهذا النوع من التوقيع عيوب أيضًا فهو محدود الانتشار بسبب التكلفة المرتفعة الناجمة عن ضرورة اقتناء أجهزة حاسوب ذات مواصفات فنية لتطبيقه، قد لا تكون في متناول الكافة، يضاف إلى ذلك أنه لا بد من التحقق من صحة التوقيع بالقلم الإلكتروني في كل مرة يتم فيها التوقيع بهذه الصورة، وذلك يتطلب تدخل طرف ثالث توكل إليه مهمة التحقق مقدّمًا من شخصية الموقع، وتسجيل نموذج لتوقيعه من أجل إجراء المطابقة، للتحقّق لاحقًا من صحة التوقيع الذي وضعه على المحرر من عدمه[2].

2. التوقيع باستخدام الخواص الذاتية (التوقيع البيومتري):

يقوم هذا الشكل من التوقيع على تكنولوجيا "العلم البيومترولوجي" المعنية باستخدام الخواص المميزة بكل شخص، وهي تدخل ضمن تكنولوجيا البصمات والخواص الحيوية والطبيعية التي تعتمد على الصفات والخواص الفيزيائية والطبيعية

---

1 عايض راشد عايض المري، مدى حجية الوسائل التكنولوجية الحديثة في آليات العقود التجارية، رسالة دكتوراة 1998م، غير منشورة، جامعة القاهرة، ص 112،113، سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، 2007م، ص226، خالد ممدوح إبراهيم، مرجع سابق، ص 200.

2 سمير حامد عبد العزيز الجمال، مرجع سابق، ص227.

والسلوكية، وتختلف هذه الصفات والخواص من شخص إلى آخر، فهي خصائص ذاتية يمكن تحديد هوية الأشخاص من خلالها.

ويتطلّب استخدام هذه الطريقة في التوقيعات الإلكترونية، أخد صورة دقيقة من الخواص مثل بصمة الأصابع، وبصمة الشفاه، ونبرة الصوت، ودرجة ضغط الدم، وشبكية العين وغيرها من الصفات الجسدية والسلوكية وتخزينها بصورة مشفرة بذاكرة الحاسوب لدى جهة مختصّة، تتولى مهمة الاحتفاظ بسجل عن الشخص يتضمّن الخصائص البيومترية المميّزة له، حتى يمكن الرجوع إليها عند الحاجة، والهدف من تشفير تلك الخواص حتى لا يستطيع أيّ شخص اختراق نظم المعلومات ومحاولة العبث بتلك البيانات أو تغييرها، مع إمكانية إعادة فكّ الشفرة عند الحاجة[1].

وعندما يرغب أيّ شخص في التعاقد عبر الإنترنت في توقيع المحرّر المثبت لهذا التعاقد باستخدام هذا الشكل من التوقيع، تقوم الجهة التي يحتفظ لديها بسجل للخواص البيومترية بإجراء عملية المطابقة لمستخدم التوقيع مع الصفات والخواص التي تم تخزينها على جهاز الحاسوب، وإذا تبيّن هناك اختلاف بينهما مهما كان بسيطًا فلا يمكن الدخول على سجل الخواص البيومترية.

لذلك هذا النوع رهين بتأمين الثقة في إيجاد التكنولوجيا التي تؤمن انتقاله بدون القدرة على التلاعب، لأنه ثبت في العمل إنه يمكن أن تخضع الذبذبات الحاملة لنبرة الصوت أو بصمة الإصبع للتزوير سواء، بطريق النسخ وإعادة الاستعمال، أم بإدخال تعديلات عليها، فمثلاً يمكن تقليد بصمة الإصبع باستخدام بصمات بلاستيكية

---

1 خالد ممدوح إبراهيم، مرجع سابق، ص 201، سمير حامد عبد العزيز الجمال، مرجع سابق، ص224.

أو مطاطية، كما يمكن تسجيل بصمة الصوت وإعادة بثّها، بالإضافة إلى ذلك يؤخذ على استخدام التوقيع البيومتري تكاليفه الباهظة، حيث يحتاج إلى إمكانيات مادية ضخمة من أجل تمكين مستخدمي تقنيات الاتصال الإلكتروني من استخدامه[1].

والجدير بالذكر أنّ التوقيع البيومتري بالرغم من أنه يمكن أن يسمح بتحديد هوية صاحب التوقيع، فإنّه لا يضمن بالضرورة التعبير الصحيح عن الرضا الموقع بالالتزام بمضمون ما تم التوقيع عليه، لأنه قد لا يتوفر لديه نية التوقيع رغم إتمامه، فمثلاً قد يجبر الشخص على الوقوف أمام الجهاز بعمل مسح الخواص البيومترية، ومن ثم أخذ بصمته دون رضاه؛ أي: تحت التهديد والإكراه، وفي هذه الحالة يكون التوقيع الناتج عن تلك العلمية رغم تحديده لهويته ناشئًا عن إرادة غيره حقيقته[2].

ومع ذلك يمكن سدّ شكوك احتمالات التزوير والوثوق في التوقيع البيومتري، من خلال تأمين نظام معلوماتي آمن يوفر الحماية والأمن، وعن طريق الاستعانة بجهات معتمدة مرخّص لها بالتصديق عليه، تخضع لرقابة الدولة أو أن تدار تحت إشرافها، حيث تضمن التحقّق من شخصية الموقع والحفاظ على سرية هذا التوقيع وحمايته[3].

3. التوقيع الرقمي:

---

1 سمير حامد عبد العزيز الجمال، مرجع سابق، ص225، سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته – صورة – حجيته في الإثبات بين التدويل والاقتباس، دار الجامعة الجديدة عام 2004م، الإسكندرية، ص71.

2 تامر محمد سليمان الدمياطي، مرجع سابق، ص 349.

3 سمير حامد عبد العزيز الجمال، مرجع سابق، ص225. سعيد السيد قنديل، مرجع سابق، ص71.

يتمّ إعداد التوقيع الرقمي من خلال تحويل المحرر والتوقيع من نمط الكتابة العادية إلى معادلة رياضية وأرقام عن طريق استخدام العمليات الحسابية واللوغارتيمات، بحيث يتم إعادة المحرّر قبل تصديره للمرسل إليه في شكل يختلف عن البيانات والمعلومات الأصلية الواردة به، مع ربط هذا المحرر بمفتاح معين، على نحو لا يمكن لأيّ شخص أن يعيده إلى صياغته المقروءة عدا الشخص المستلم وحده من خلال فك التشفير المطلع عليه[1].

والجدير بالذكر تشمل عملية تحويل المحرر العرفي بطريق التشفير، الكتابة والتوقيع في آن واحد، وذلك بتغيير المعلومات والبيانات مضمون المحرر إلى رموز غير مفهومة، بالإضافة إلى تحويل التوقيع المؤشر به على المحرر نفسه إلى خطيًّا- هو الآخر- إلى أرقام يستوي أن يكون التوقيع التقليدي في صورة إمضاء بخط اليد أو بصمة إصبع، ولكن بمجرد تشفير المعلومات والتوقيع لا يستطيع الأشخاص غير المرخص لهم من الاطلاع على تلك المعلومات فهم تلك الرموز والأرقام، لأنه لا يمكنهم استخدام مفتاح فك التشفير الذي يعيد المعلومات المشفرة والتوقيع الرقمي إلى صيغتيهما الأصلية، فالتشفير هو الذي يكفل سرية التوقيع الرقمي، والذي يمثل الوسيلة الأساسية لضمان توفير الثقة والأمن للمعاملات المنعقدة عبر شبكة الاتصالات المفتوحة "الإنترنت".

وينشأ التوقيع الرقمي ويتم التحقّق من صحته باستخدام التشفير[2]، فمثلاً إذا أراد الموقع إرسال رسالة عبر شبكة الإنترنت فيقوم بتحويلها إلى رموز أو معادلة

---

1 سعيد السيد قنديل، مرجع سابق ص72.

2 خالد ممدوح إبراهيم، مرجع سابق، ص199.

رياضية غير مفهومة، ويجب أن يضيف توقيعه عليها، وذلك بتشفيره وإضافة أرقام تمثّله، ثم إرسالها للشخص المرسل إليه، وفي هذه الحالة يستطيع المرسل إليه استلام الرسالة، والتحقق من صحة التوقيع الرقمي باستخدامه مفتاح فك التشفير الذي يكون على علم به ويطلق عليه بالمفتاح العام، أمّا إذا أراد المرسل إليه التحقق من سلامة الرسالة، فإنه يستخدم برنامج التشفير نفسه لإنشاء رسالة أخرى، تم يقارن بينهما فإذا كانتا متطابقتين فهذا دليل على أن الرسالة وصلت إليه دون تغيير، أمّا إذا تبيّن أنّ هناك اختلاف بين الرسالة المستلمة، والرسالة التي أنشأها المرسل إليه، فإنّ ذلك يعني أنه قد تم اختراق مفتاح فك تشفيرها من الغير (القراصنة)، ولحق بها تعديل أو تحريف بعد إرسالها إلى المرسل إليه[1].

ويرتبط التوقيع الرقمي بالتشفير ارتباطًا عضويًّا، والتشفير هو عملية تغيير في بيانات الرسالة وتحويلها إلى مجموعة من الأرقام والرموز، وفيما يخصّ التوقيع الرقمي فإنّ أسلوب التشفير السائد يتحدّد في نوعين: أولهما يسمى بالمفتاح المماثل أو المفتاح العام[2]، وفي هذا النوع من التشفير يستخدم كلّ من المرسل والمستقبل ذات المفتاح السري لتشفير الرسالة، وفكّ تشفيرها، بحيث يستطيع المرسل إليه عند استلامه الرسالة المشفرة فك الشفرة وإعادة تحويلها إلى شكلها الأصلي المفهوم، ومن تم التعرف على هوية المرسل ومضمون الرسالة، ويتطلب هذا النوع من التوقيع منذ البداية اتفاق كل من المرسل والمرسل إليه على مفتاح الشفرة الذي سيتم استخدامه ويستلزم المحافظة على سرية هذا المفتاح طوال فترة استخدامه، لأنّ من أهم عيوب هذا النوع من التشفير تكمن في عملية تبادل المفتاح بين أطراف التعامل، وقد يؤدّي ذلك إلى تسرّب مفتاح

---

1 خالد ممدوح إبراهيم، مرجع سابق، ص199.

2 خالد ممدوح إبراهيم، مرجع سابق، ص199.

فكّ الشفرة واختراقه على أيدي القراصنة والمنافسين، غير أنّ هذا المفتاح لا ينتج أيّ أثر قانوني إلا مع المفتاح الخاص.

أمّا بالنسبة للطريقة الثانية يستخدم في التشفير مفتاحان: أحدهما خاص، والآخر مفتاح عام[1]، مرتبطين معًا في عملهما وكلّ منهما يكمل الآخر، ولكن من غير الممكن التعرّف على أحد المفتاحين من خلال المفتاح الآخر، حيث يتركّب المفتاح الخاص[2]، من مجموعة من الرموز والأرقام التي يمكن تخزينها على بطاقة إلكترونية، ويتم الوصول إليه عن طريق الرقم الشخصي لصاحبه، ولا يكون هذا المفتاح معروفاً إلا للموقع فقط أو المرسل والذي يظل، محتفظًا بسريته باستمرار، بحيث يكون هو الوحيد فقط القادر على الدخول عليه واستخدامه وفك السرية "**الشفرة**"، ويستخدم هذا المفتاح لتشفير الرسالة وفكّ شفرتها، أمّا المفتاح العام فإنّه يتكوّن أيضًا من رموز وأرقام، ويكون متاحًا للمتعاقد الآخر.

---

1 سمير حامد عبد العزيز جمال، مرجع سابق، ص219.

2 سعيد السيد قنديل، مرجع سابق، ص62.

الفصل الأول

القوة الفنية والثبوتية للتوقيع الإلكتروني

تمهيد

أدّى السماح للجمهور باستعمال شبكة الإنترنت في بدايات التسعينيات من القرن الماضي، إلى ظهور أنواع جديدة من إمكانيات الاتصال والتعامل والتعاقد. وقد أدّى بالتالي إلى إمكانية تبادل المعلومات في بداية الأمر ثم إلى تبادل الرسائل والمعلومات في وقت لاحق واستعمل كوسيلة لتسليم بعض المنتجات ذات الطابع الإلكتروني، وهو ما أصبح يعرف بالمعاملات الإلكترونية، وهنا برزت إشكالية صحة كلٍّ من المستند الإلكتروني غير المطبوع ورقيًّا والتوقيع الإلكتروني وسلامته.

إنّ طبيعة حفظ المستند الإلكتروني بصورة إلكترو–مغناطيسية تسمح بتعديله بدون أن يتمكّن من يعاينه من اكتشاف أيّ تعديل طرأ عليه منذ صياغته الأولى "الأساسية"، ومن هنا كان لا بد من وضع معايير لحماية المستند الإلكتروني، مثل التشفير والصعوبات التقنية الأخرى التي تمنع الولوج إليه، وقد تمّ كذلك وضع برمجيات قادرة على كشف أيّ خرق أو تلاعب بسلامته.

يتمتّع التوقيع الإلكتروني بعدد من الإجراءات التقنية التي تسمح باعتماده، والتأكّد من صحته ومن صدوره عن الشخص المعنيّ به، وتعرف هذه الوسائل بآليات إنشاء التوقيع الإلكتروني والتحقّق من صحّته، وفيما يأتي سأتطرّق إلى الحديث عن القوة الفنية والثبوتية للتوقيع الإلكتروني، وذلك من خلال تقسيم هذا الفصل إلى مبحثين على النحو الآتي:

المبحث الأول: آلية تشفير التوقيع الإلكتروني.

المبحث الثاني: طرق التحقّق من سلامة الرسالة والمصادقة عليها.

المبحث الأول
آليه تشفير التوقيع الإلكتروني

تمهيد وتقسيم:

تهدف عملية التشفير إلى الحفاظ على سريّة المعلومات الثابتة منها والمتحركة باستخدام برنامج له قدرة على تحويل تلك المعلومات وترجمتها إلى رموز وأرقام وحروف غير مفهومة إلا من قبل صاحبها(1).

لقد ازدادت أهمية أنظمة التشفير وتطوّرت مع زيادة حجم التبادلات عبر شبكة الإنترنت حيث تمثّل إحدى الركائز الأمنية التي توفّر الأمان والسرية للسندات الإلكترونية وتضمن سلامتها(2).

فبانعدامها تنعدم ثقة الأفراد بالمعاملات الإلكترونية والذي يزيد من ذلك، وكما هو معلوم للجميع إن المعلومات المتوفرة عبر شبكة الإنترنت متاحة للكافة ويمكن لأيّ شخص وفي أيّ وقت الاطّلاع عليها ونسخها واستثمارها لصالحه، لذلك توفّر أنظمة التشفير نوعًا من الطمأنينة والثقة للمتعاملين عبر شبكة الإنترنت فهي تهدف

1 محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2006م، ص 25.

2 عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، بيروت، لبنان، ط 1، 2010م، ص 230.

إلى التحقق من هوية الشخص الذي يتم التعامل معــه، وفيمـا إذا كانـت السـندات الإلكترونية للمعاملة قد صدرت منه، بالإضافة إلى التأكّد من إثبات صـحّتها وعـدم حصول تلاعب فيها أثناء تبادل البيانات والمستندات الإلكترونية[1].

وفيما يأتي سأتطرق إلى الحديث عن آلية التشفير من خلال المطلبين الآتيين:

المطلب الأول: تعريف تشفير التوقيع الإلكتروني.

المطلب الثاني: الجانب الفني للتشفير وصوره.

المطلب الأول: تعريف تشفير التوقيع الإلكتروني

لقد اكتشف التشفير سنة 1965م إبّان حرب الفيتنام مـن قبـل ثلاثـة علمـاء، وعرفوا علم التشفير بأنه العلم الذي يعتمد على وسائل وطرق تجعل مـن المعلومـة غير مفهومة وغير مقروءة إلا لأطرافها، حيث يتأكّد كلّ من المرسل والمرسل إليـه عدم تسليم الرسالة لطرف ثالث غيرهما، يتم الاطلاع على البيانات الإلكترونية فـي المعاملات التجارية والإدارية باستخدام مفتاحين: الأول عام معروف لعامة النـاس، أما الثاني فهو مفتاح خاص لا يعلمه سوى صاحبه، استعمال المفتاحين دلالة قاطعـة على التأكّد من هوية الأطراف الذين قد يثبت من ذلك الإجراء رغبتهما في التعاقد[2].

1 قدري عبد الفتاح الشهاوي، قانون التوقيع الإلكتروني ولائحته التنفيذية والتجارة الإلكترونية في التشريع المصري والعربي والأجنبي، دار النهضة العربية، مصر، 2005م، ص 413 – 414.

2 عبد الرسول عبد الرضا، محمد جعفر هادي، المفهوم القانوني للتوقيع الإلكتروني، دراسة مقارنة، مجلة المحقّق الحلي للعلوم القانونية والسياسية العدد الأول/ السنة الرابعة، ص 15.

الفرع الأول: التعريف التشريعي للتشفير

ذكر تعريف التشفير في مشروع قانون التجارة الإلكتروني المصري بأنّه تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها[1].

وعرّفته المادة (9/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم (15) لسنة 2004 بقرار وزير الاتصالات رقم (109) لسنة 2005م بأنه (منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة)[2].

وعرف التشفير أيضًا قانون رقم (83) لسنة 2000م بشأن مبادلات التجارة الإلكترونية التونسية بأنه عبارة عن "استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها"[3].

ونصّت المادة (1) من قانون التجارة الإلكتروني البحريني الصادر في 2002/9/14 على أنه "بيانات إنشاء توقيع بيانات فريدة تستعمل لإنشاء توقيع إلكتروني كالرموز أو مفاتيح التشفير الخاصة".

---

1 المادة الأولى من مشروع التجارة المصري لسنة 1999م.

2 المادة (1/ 9) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم (15) لسنة 2004.

3 الفصل الثاني من قانون المبادلات والتجارة الإلكترونية التونسي رقم (83) لسنة 2000.

أمّا في التشريع العراقي فإنّ المشرع العراقي في بادئ الأمر لم يتطرّق إلى موضوع التشفير بصورة مباشرة وإنّه اكتفى بما أورده حول التوقيع الإلكتروني، وذلك في الفصل الثالث ضمن قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2010م، حيث إنّ (التوقيع الإلكتروني) يرتكز في الأساس على عملية التشفير، كما أنه يعتبر أحد الضمانات والطرق التي توفّر الحماية للتعاملات والتصرفات التي تتم من خلال الإنترنت والوسائل الإلكترونية الأخرى لكنه عاد وعرفه فيما بعد بنص صريح ضمن قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012[1].

أمّا المشرع المغربي من خلال قانون (53.05) المتعلّق بالتبادل الإلكتروني للمعطيات القانونية فقد تطرق بدوره إلى تقنية التشفير، حيث خصّص لها الفرع الثاني من الباب الأول من القسم الثاني، وذلك تأكيدًا على دورها وعلى أهميتها.

---

1 من قانون تصديق اتفاقية تنظيم أحكام التوقيع الإكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012م، منشور في مجلة الوقائع العراقية بالعدد 4274 في 15/ 4/ 2013م، والتي تنص على أنّ ((التشفير: منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًّا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة)).

ويراد بوسيلة التشفير كلّ عتاد أو برمجية أو هما معًا، ينشأ أو يعدل من أجل تحويل معطيات سواء كانت عبارة عن معلومات أم إشارات أم رموز، استنادًا إلى اتفاقيات سرية، أو من أجل إنجاز عملية عكسية لذلك بموجب اتفاقية سرية أو بدونها[1].

وقد أخذ المشرع الفرنسي بنظام التشفير ضمن قانون تنظيم الاتصالات عن بعد رقم (90) لعام 1990 المعدل حيث عرفه بأنه ((جميع الوسائل المعتمدة بالاتفاقيات السرية والتي تحوّل المعلومات أو الإشارات المفهومة أو المقروءة باستخدام معدات أو برامج الحاسب الآلي التي تكون مهمة لهذه الغاية، إلى معلومات وإشارات غير مقروءة أو أرقام بالعملية المعاكسة))[2].

وقد أجاز المشرع الفرنسي استخدام التشفير ولكن تحت مراقبة وإجراءات صارمة وخاضعة لرقابة الدولة، وذلك في قانون تنظيم الاتصالات الفرنسي عن بعد رقم (90) لسنة 1990 ثم جاء بعد ذلك قانون الاتصالات رقم (96 – 659) لسنة 1996 ليعدل أحكام القانون السابق ويجعل استخدام وسائل التشفير حرًّا بشرط استيفائها شروطًا محدّدة، كذلك بيّن قانون 1996 شرط استيراد وتصدير برامج التشفير حيث جعلها مقيّدة بشرط الحصول على تصاريح وإجازات مسبقة لكنه بالوقت نفسه خفّف من إجراءات الحصول على تلك التصاريح والإجازات بهدف التخفيف من الشكلية المشدّدة التي اعتمدها القانون، وفي عام 1998م صدرت وثيقة تتضمّن شرحًا تطبيقيًّا لنظام التشفير الذي جاء بقانون عام 1996م، إذ سمح هذا

---

1 التعريف الذي أورده المشرع المغربي لوسيلة التشفير من خلال المادة (12) من القانون المتعلّق بالتبادل الإلكتروني للمعطيات القانونية رقم 53.05.

2 المادة (28–1) من القانون الفرنسي لتنظيم الاتصالات عن بعد رقم (90) لسنة 1190 والمعدل بموجب القانون رقم (575) لسنة 2004.

القانون باستخدام تقنيات التشفير ووسائله التي تؤمن وظائف المصادقة على السندات الإلكترونية، وكذلك الوسائل التي تؤدّي وظيفة السرية؛ (أي: الوسـائل التـي تقـوم بتشفير السندات الإلكترونية)[1].

الفرع الثاني: التعريف الفقهي للتشفير

إنّ التشفير إجراء يؤدّي إلى توفير الثقة في المعاملات الإلكترونية، وذلك باستخدام أدوات أو أساليب لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها غير المشروع، ويسمح نظام التشفير بتلافي بعض المخاطر المتوقّعة من استخدام الطرق الإلكترونية في المعاملات التجارية، حيث يتمّ التأكّد عن طريقه من أن المعلومات التي تسلّمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها، بحيث يتأكّد المرسل إليه الذي يستطيع عن طريق استخدام وسائل فنية الاطلاع على محتوى المعلومة[2].

ويعرّف التشفير بأنه تمويه للرسالة بطريقة تخفي حقيقة محتواها وتجعلها رمزًا غير مقروء، ولذلك فإنها تسمى أيضًا بعملية الترميز[3].

ويعرّف التشفير بأنه عملية تمويه للرسالة الإلكترونية أو السند الإلكتروني بطريقة تخفي حقيقة محتواه من خلال تحويله إلى رموز وإشارات لا يمكن فهمها إلا بعد القيام بفكّ الشفرة[1].

---

1 عباس العبودي، مرجع سابق، ص 236 وما بعدها.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 245.

3 عمر حسن المومني، التوقيع الإلكتروني والتجارة الإلكترونية، الطبعة الأولى، دار وائل للنشر، عمان، الأردن، 2003م، ص 54.

والهدف من عملية التشفير هو توفير أمن المتبادل والمتبادلين في شبكة الإنترنت، والتأكّد من هوية مطلق الرسالة وتوفير الحماية الخصوصية وسرّيّة المعلومات في التجارة الإلكترونية[2].

وقد عرّفه الفقه بأنه عملية تحويل النص إلى رموز وإشارات غير مفهومة، تبدو غير ذات معنى لمنع الغير من الاطلاع عليها إلا للأشخاص المرخّص لهم[3].

ونلاحظ تفاوت التشريعات المنظمة للتجارة الإلكترونية في مواقفها من تنظيم أحكام التشفير بين من نظّمها جزئيًّا وبين من أشار إليها فقط بصورة عرضية، وبين من أغفلها تمامًا مثل قانون دبي بشأن المعاملات والتجارة الإلكترونية[4].

لذلك تحتوي عملية التشفير بكلّ سهولة على تحويل النصوص العادية الواضحة إلى نصوص مشفّرة غير مفهومة، وهي مبنية على مفهوم أساسي مفاده أنّ كلّ معلومة مشفرة تحتاج لفكّها وإعادتها إلى وضعها الأصلي[5].

وتتم عملية التشفير من خلال استعمال مفاتيح خاصّة في تشفير البيانات وفك تشفيرها، ويتم التوصّل إلى هذه المفاتيح من خلال تطبيق معادلات ودوال رياضية

---

1 محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2005م، ص 159.

2 هادي مسلم يونس قاسم البشكاني، التنظيم القانوني للتجارة الإلكترونية، دراسة مقارنة، أطروحة دكتوراه مقدمة إلى مجلس كلية القانون في جامعة الموصل، 2002م، ص 281.

3 محمد أمين الرومي، مرجع سابق، ص 25.

4 آزر دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2016م، ص88.

5 محمد السعيد رشدي، التعاقد بوسائل اتصال حديثة، منشأة المعارف، الإسكندرية، مصر، 2005م، ص 205.

(خوارزميات) معقدة جدًّا بهدف تصعيب الأمر على كلّ من يحاول حلّ المعادلات والتوصّل إلى المفتاح الخاص بفك الشفرة بطريق غير مشروع، وذلك لأنّ المفتاح عبارة عن سلسلة من الأرقام أو الحروف يتم التوصّل إليها من خلال نتائج حلّ المعادلة الرياضية، حيث إنّ المعادلة الرياضية (الخوارزمية) وطول مفتاح التشفير يعتبران من أهم العوامل التي تجعل عملية التشفير قوية وفعّالة[1].

ولتحقيق الأهداف المرجوة منه، فإنّ التشفير يتم على مستويات عديدة منها:

تشفير وصلات الاتصالات:

ويستخدم هذا النوع من التشفير لتأمين كلّ ما يمرّ عبر وصلات الاتصالات عند نقطة الإرسال، ويتم حلّ الشفرة عند نقطة الاستقبال، ومن نماذج تطبيقاته ما يسمى بالشبكات الخاصة المؤمنة[2].

مستوى التصفّح:

ويستخدم هذا المستوى في تشفير البيانات التي يتمّ تداولها بين برامج تصفّح البيانات وبين مقرّ المعلومات، ومن تطبيقات هذا النظام، نظام تأمين بروتوكول الاتصال "HTTPS" [3]

---

1 محمد فواز المطالقة، مرجع سابق، ص 162.

2 رأفت رضوان، عالم التجارة الإلكترونية، منشورات المنظمة العربية للعلوم الإدارية، القاهرة 1999م، ص82.

3 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 262.

مستوى التطبيق المستخدم في تنفيذ المعاملة الإلكترونية:

ويستخدم كتطبيق خاص لتشفير البيانات، كما يتم استخدامه للتشفير الجزئي، ومن نماذج تطبيقاته نظام تأمين المعاملات الإلكترونية " Set " وهي اختصار لعبارة Secure Electronic transaction وكذلك نظام محفظة سبيركاش Cyber cash wollet [1].

مستوى الملفات:

ويستخدم هذا المستوى لأجل تشفير الملفات والرسائل التي يتم تبادلها كما في الحكومة الإلكترونية، ومن تطبيقات مستوى التشفير المذكور نظام نورتل إنترست Nortel's entrust، وكذلك نظام يسمى زيمرمان للخصوصية Philezimmerman's pertly quad privacy CPGP [2].

المطلب الثاني: الجانب الفني للتشفير وصوره

أظهرت المعاملات المالية على الإنترنت، الحاجة لتوفير الحماية، وذلك عن طريق شخص ثالث ليس من أطراف العقد حتى يوثق البيانات المتبادلة وبصفة خاصة التوقيع الإلكتروني، ويشهد بصحته دون أن يكون له مصلحة شخصية في هذه البيانات[3].

---

1 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 262.

2 رأفت رضوان، مرجع سابق، ص82 .

3 مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، 2001م، ص22.

ولذلك يعدّ التشفير من وسائل حفظ المعلومات وسريتها في نطاق الأنظمة الإلكترونية لا سيما في الحكومة الإلكترونية وتطبيقاتها، كما في التجارة الإلكترونية والتي تتطلب الحفاظ على بيانات ومعاملات الأطراف وحجم الصفقات ونوعها، وكذلك حماية النقود المتداولة في نطاق هذه التجارة[1].

ويهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات، ومن ثمّ منع وصولها أو وصولها مشوّهة إلى الطرف الآخر في المعاملة التجارية، وذلك على نحو يعرقل هذه التجارة، وفي كلّ الأحوال لا بد من حماية الرسالة وضمان وصولها بالشكل المطلوب إلى مستقبل هذه الرسالة.

والمشرع الفرنسي بدوره وبمقتضى قانون صدر في عام 1990م، أعطى المشروعات الصغيرة الحق في تشفير رسائلها ومعلوماتها بعد أن كان ذلك مقصورًا على المجالات العسكرية والدبلوماسية والحكومية[2].

الفرع الأول: الجانب الفني للتشفير

إنّ الطريقة الشائعة للتشفير تتمثّل بوجود مفتاحين، المفتاح العام public-key وهو معروف للكافة، ومفتاح خاص private-key ، يتوفر فقط لدى الشخص الذي أنشأه، ويمكن بهذه الطريقة لأيّ شخص يملك المفتاح العام أن يرسل الرسائل المشفرة، ولكن لا يستطيع أن يفك شيفرة الرسالة إلا الشخص الذي لديه المفتاح

1 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 260.

2 نفس المرجع سابق، ص 242.

الخاص[1].

إنّ استخدام التوقيعات الإلكترونية عادة يتضمّن عمليتين؛ واحدة يتم إنجازها من قبل الموقع، والأخرى من قبل مستلم التوقيع الإلكتروني[2]:

1. إنشاء التوقيع الإلكتروني يستخدم نتيجة هاش يتم اشتقاقها منه، وتكون مقتصرة على كل من الرسالة الموقعة ومفتاح خاص معين بغرض أن تكون نتيجة الــ هاش آمنة ومحكمة يجب ألاّ يكون هناك إمكانية أو احتمال ضئيل فقط بأن نفس التوقيع الإلكتروني يمكن إنشاؤه من خلال تركيبة أيّ رسالة أخرى أو مفتاح خاص آخر.
2. التثبّت من صحة التوقيع الإلكتروني: وهي عملية التأكّد من التوقيع الإلكتروني من خلال الرجوع إلى الرسالة الأصلية وإلى مفتاح عام معين، وبهذا يتمّ تحديد ما إذا كان التوقيع الإلكتروني قد تم إنشاؤه لتلك الرسالة باستخدام المفتاح الخاص المقابل للمفتاح العام المشار إليه.

ممّا تقدم تظهر العلاقة بين التوقيع الإلكتروني والتشفير، فالتوقيع الإلكتروني هو ختم رقميّ مشفّر، يملك مفتاحه صاحب الختم، ويعني تطابق المفتاح مع التوقيع الرقمي على الرسالة الإلكترونية على أنّ مرسل الرسالة هو من أرسلها فعلاً، وليست مرسلة من قبل شخص آخر، ويضمن التوقيع الرقمي عدم تعرّض الرسالة لأيّ نوع من أنواع التعديل، بأي طريقة. لذلك يعتبر التشفير إجراءً تقنيًّا يسمح

1 أمير فرج يوسف، الجديد في التوقيع الإلكتروني لدول الخليج العربي والحجية القانونية للتوقيع الإلكتروني في كافة المعاملات الإلكترونية، دراسة قانونية مقارنة بالدول العربية والأجنبية، دار الكتب والدراسات العربية، الإسكندرية، 2015م، ص 286.

2 عبد الرسول عبد الرضا، محمد جعفر هادي، مرجع سابق، ص 14.

بزيادة الأمان والثقة في التجارة الإلكترونية، ويضمن السرية الكاملة في ذلك والحيلولة دون تعديلها أو اختراقها.

وتتلخّص أغراض التشفير في الآتي[1]:

أ. **توثيق الموقّع:** في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معيّن ومحدّد فإنّ التشفير ينسب ويعزو الرسالة إلى الموقع. ولا يمكن تزوير التوقيع الإلكتروني ما لم يفقد الموقع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر) كأن يقوم بإفشائه أو يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية.

ب. **توثيق الرسالة:** كذلك فإنّ التشفير يعمل على تحديد هوية الرسالة الموقّعة بثقة ودقّة ويقين أكثر من التوقيعات على الورق، وإنّ عملية التثبّت من الصحة تكشف أيّ تلاعب، حيث إنّ أيّ مقارنة بين العملية الواحدة يتم إعدادها عند التوقيع والأخرى عند التثبّت من الصحة تبيّن ما إذا كانت الرسالة هي نفسها عندما تم توقيعها.

مستوى عالٍ لضمان أنّ التوقيع الإلكتروني هو للموقّع بدون تكلّف أو رياء. مقارنة مع الأساليب الورقية مثل بطاقات نموذج اعتماد التوقيع، والتي هي أساليب مملّة وتستغرق الكثير من الجهد بحيث إنه نادرًا ما يتم استخدامها بالواقع – فإنّ التوقيعات الإلكترونية تعطي وتولد درجة ضمان أعلى بدون أن تضيف كثيرًا على الموارد المطلوبة للمعالجة.

---

1 عبد الرسول عبد الرضا، مرجع سابق، ص 15.

ومن ملاحظة ما تقدّم يتبيّن لنا مدى الحماية التي يوفّرها التشفير في حماية من يقوم بإجراء المعاملات عبر شبكة الإنترنت بشكل عام، حيث إنه يعتبر من أهم الضمانات، لما يهدف إليه من الحفاظ على سلامة المعلومات والمعطيات الإلكترونية وتأمين خصوصيتها وشرعيتها، بالإضافة إلى حماية المشتري عند قيامة بعملية السداد النقدي سواء من خلال تأمين عملية تحويل الأموال أم من خلال تأمين أرقام بطاقات الائتمان عند إرسالها لاستقطاع الثمن[1].

الفرع الثاني: طرق التشفير وصوره

هناك أربعة أنواع أو أنظمة أو صور للتشفير كشف عنها التطور التكنولوجي وصناعة تكنولوجيا المعلومات، والتي يتم استخدامها في التجارة الإلكترونية ومختلف التعاملات التي تتم عبر الإنترنت، وهما:

1. التشفير بالمفتاح المتماثل:

في هذا النوع من أنواع التشفير يتم استخدام مفتاح واحد يعرف (بالمفتاح الخصوصي) لتشفير البيانات وفك تشفيرها، حيث يتم من خلال قيام مرسل البيانات بتشفيرها وإرسالها، ومن ثم يقوم بإرسال المفتاح الذي استخدمه في التشفير بطريقة مؤمنة إلى متلقي الرسالة[2].

---

1 طاهر شوقي مؤمن، عقد البيع الإلكتروني، دار النهضة العربية، مصر، 2007م، ص 102.
2 عمر حسن المومني، مرجع سابق، ص 55.

وقد نلاحظ من هذه الطريقة أنّ المفتاح السرّيّ يرسل من المرسل إلى المرسل إليه بطريقة آمنة إذا كانت هذه الطريقة الآمنة موجودة، فلا حاجة إلى تشفير الرسالة، ويمكن إرسالها غير مشفرة[1].

لكن ما يؤخذ على هذا النوع من التشفير أنّ المفتاح المستخدم قد يتسرّب إلى الغير أثناء عملية تبادليه خاصّةً مع توجّه غالبية المتعاملين عبر الإنترنت إلى ذلك، ويجب أن يمتلك المرسل إليه عددًا من المفاتيح الخصوصية يوازي عدد السندات الواردة إليه من مصادر مختلفة[2].

وغالبًا ما تستعمل هذه الطريقة في البنوك لتشغيل الصراف الآلي، ويعتمد مفهوم التشفير المتماثل على معيار تشفير البيانات اعتمادًا على الخوارزمية التي تستخدم مفتاحًا بطول (56bit)[3].

وأيضًا من المشاكل التي تواجه هذا النوع من التشفير أنّ المتنصت يستطيع تخزين المعلومات على الرغم من كونها مشفرة، وذلك لتوفرها على كل جهاز، وبينما هو مستمر في مراقبتها وتخزينها، يحاول الحصول على المفتاح بطرق أخرى مثل اختراق جهاز المرسل أو جهاز المستقبل، وعند الحصول على المفتاح فإن كافة البيانات التي تم تبادلها في السابق والتي تنشر بعد ذلك ستكون مكشوفة، وقد تترتب على ذلك نتائج خطيرة[4].

---

1 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 260.

2 عباس العبودي، مرجع سابق، ص 232.

3 آزاد دزه يي، مرجع سابق، ص 97.

4 محمد فواز المطالقة، مرجع سابق، ص 164.

ولتجاوز هذه المشاكل من المستحسن تغيير هذا المفتاح بصفة دورية، بحيث لا تكون هنالك كمية كبيرة من البيانات الحساسة تعتمد على مفتاح واحد، لكن من الصعب تغيير المفتاح بصفة دورية إذا لم تكن هنالك طريقة آمنة وسهلة وعملية لإعلام الأطراف بمفتاح تشفير جديد. ويمكن استخدام تقنية التشفير بالمفتاح المتماثل لتشفير المعلومات على القرص الصلب، إذا لم يرد الشخص إتاحة الفرصة للجميع كي يطّلعوا على محتوياتها، ولكن تتكرّر هنا مشكلة حساسية مفتاح التشفير، فيجب أن يتم تخزين المفتاح المستخدم للتشفير في مكان منفصل تمامًا عن البيانات المشفّرة، لأنّ إغفال ذلك سيسهّل فكّ شفرات هذه الملفات[1].

2. التشفير اللا متماثل أو الهندسة العكسية (المفتاح العام والخاص):

وأمّا الطريقة الثانية للتشفير، فهي طريقة (الهندسة العكسية) ويستخدم فيها مفتاحان: أحدهما عام والآخر خاص، وكلاهما له علامات رياضية معقّدة لا يعرفها إلا صاحب المفتاح ذاته، والمفتاح الخاص لا يعرفه سوى صاحبه ولا يمكن لآخر معرفته، أمّا المفتاح العام ففي كلّ الحالات يكون معلومًا للجمهور[2].

فنظرًا للعيوب التي ظهرت في نظام التشفير المتماثل لجأ علماء الرياضيات وخبراء صناعة تكنولوجيا المعلومات إلى البحث عن نظام جديد يحلّ محلّه ويؤدّي الغاية المرجوّة منه على أفضل وجه، وبالفعل تمّ التوصّل إلى نظام التشفير غير المتماثل على يد علماء الرياضيات (Shamir and Adleman،Rivest) في

---

1 آزاد دزه يي، مرجع سابق، ص 98.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 211.

أمريكا عام 1978م، ويعتمد هذا النظام على وجود مفتاحين عام وخاص تربطهما علاقة رياضية متينة، وقد عرف المشرع المصري هذا النظام في المادة (1/ 10) من قرار وزير الاتصالات وتكنولوجيا المعلومات رقم (109) لسنة 2005 بأنه ((منظومة تسمح لكلّ شخص طبيعي أو معنوي بأن يكون لديه مفتاحان متفردان؛ أحدهما عام متاح إلكترونيًّا، والثاني خاص يحتفظ به الشخص على درجة عاليه من السرية)).

كما عرف المفتاح العام بأنّه أداة إلكترونية متاحة للكافة تنشأ بواسطة عملية حسابية خاصة، وتستخدم في التحقّق من شخصية الموقع على المحرر الإلكتروني، والتأكّد من صحة محتوى المحرر الإلكتروني الأصلي وسلامته[1].

وعرف المفتاح الخاص بأنه أداة إلكترونية خاصة بصاحبها تنشأ بواسطة عملية خاصة، وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية، ويتم الاحتفاظ بها على بطاقة ذكية مؤمنه[2].

ومن خلال ما تقدّم تبيّن التعاريف المذكورة آلية العمل بموجب هذا النوع من التشفير، حيث إنّ كل مستخدم للإنترنت يرغب في استعمال التشفير في تعاملاته يجب أن يملك مفتاحين: أحدهما عام يكون متاحًا لمن يرغب بالتعامل مع صاحب المفتاح، والآخر يحتفظ به لنفسه ويكون محفوظًا على بطاقة ذكية مؤمنة.

---

1 المادة (1/ 11) من قرار وزير الاتصالات وتكنولوجيا المعلومات المصري رقم (109) لسنة 2005.

2 انظر المادة (1/ 12) من قرار وزير الاتصالات وتكنولوجيا المعلومات المصري، المرجع السابق.

فمن يريد أن يتعامل مع صاحب المفتاح يقوم بتشفير الرسالة بواسطة المفتاح العام ومن ثم يقوم المرسل إليه بفك تشفير الرسالة بواسطة مفتاحه الخاص الذي يكون بدورة متزامناً مع المفتاح العام وبالتالي يتفرد بقراءة ما ورد إليه من معلومات[1] .

ويلاحظ على هذا النوع من التشفير أنه يمتاز بنوع من التعقيد حيث إنه يحتاج إلى وقت أطول من سابقه (التشفير المتماثل) للقيام بعملية التشفير، ويحتاج إلى الوقت نفسه لفك التشفير، لذلك تم ابتكار طريقة المزج بين النوعين من خلال استخدام نظام التشفير غير المتماثل وتشفير الرسالة بمفتاح خاص ثم تشفير المفتاح الخاص بمفتاح عام وإرساله مع الرسالة عبر أية وسيله للاتصال[2].

إنّ التشفير بهذه الطريقة يحتاج إلى وقت أطول وهذا البطؤ في العملية لا يتوافق مع هدف التجارة الإلكترونية التي تمتاز بالسرعة، ويعدّ هذا النظام نموذجًا محسنًا ومطورًا. علمًا بأنّ المفتاح العام العلني يستخرج من علاقة رياضية للمفتاح الخاص السري ذات اتجاه واحد بحيث لا يمكن استخراج المفتاح الخاص من المفتاح العام[3].

ثالثًا: المزج بين نظامي المفتاح العام والمتماثل

من الأكيد أنّه يمكن العمل بطريقتي التشفير معًا في إرسال خطاب سري وموقع في الوقت نفسه[4]، حيث يختصّ مقدّمو خدمات المصادقة الإلكترونية المعتمدون لهذا

1 عباس العبودي، مرجع سابق، ص 233. محمد فواز المطالقة، مرجع سابق، ص 165.

2 قدري عبد الفتاح الشهاوي، مرجع سابق، ص 416.

3 علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر والتوزيع، عمان الأردن، 2005م، ص 38.

4 الأستاذ العربي جنان، مرجع سابق، الصفحة 40.

الغــرض[1]، باعتماد تقنية التشفير من خلال التأكيد على نسبة المعلومات لصاحبها وبالتالي ضمان سرية تبادل المعطيات، وإن تعذر ذلك تعيّن أن يكون الأشخاص الراغبون في تقديم خدمات التشفير الخاضعة للترخيص معتمدين لهذا الغرض من لدن الإدارة.

وتقوم هذه الطريقة على المزج بين النظامين لتحقيق درجة تأمين عالية في أقل وقت ممكن، وذلك باتّباع الخطوات الآتية:

أ. الرسالة الأصلية من المرسل إلى المرسل إليه تشفّر بالطريقة السيمترية أو المفتاح الخاص.

ب. المفتاح المتماثل –السيمتري– يشفّر بدوره عن طريق المفتاح العام للمرسل إليه public Key.

ج. يتم إرسال الرسالة المشفّرة باستخدام المفتاح المتماثل والمفتاح المتماثل المشفر بأيّ وسيلة اتصالات عادية.

د. حين يتلقّى المرسل إليه مفتاح التماثل المشفر – بالمفتاح العام الخاص به يقوم بفكّ شفرة المفتاح المتماثل المشفر باستخدام المفتاح الخاص به، وبذلك يحصل على المفتاح المتماثل الذي شفرت به الرسالة الأصلية.

ه. يقوم المرسل إليه، بعد فكّ شفرة المفتاح المتماثل، في استخدام هذا المفتاح الأخير في فك الرسالة المشفّرة حتى يحصل على الرسالة الأصلية[2].

---

1 لمعرفة الشروط الواجب توفرها في مقدّمي خدمات المصادقة الإلكترونية، يرجى مراجعة المادة (21) من القانون المتعلّق بالتبادل الإلكتروني للمعطيات القانونية.

2 رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص 89.

رابعًا: نظام المعاملات الإلكترونية الآمنة (SET)

يفيد هذا النظام في الأعمال المالية للحكومة الإلكترونية، وقد تم تطويره بالاتفاق والتعاون بين شركتي فيزا كارد وماستركارد، وذلك بغرض تأمين المعاملات المالية على شبكة الإنترنت عن طريق استخدام بطاقات التأمين.

وظهر ذلك النظام كثمرة تعاون بين شركتي ماستركارد مع شركة (IBM) وشركة نيت سكيب لبناء نظام خاص لتشفير بروتوكولات الدفع تحت اسم(SEPP)[1].

وفي عام 1996م صدر النظام الجديد المشترك للمعاملات الإلكترونية الآمنة، وأصبح هذا النظام هو النظام الأول الآمن المقرّر بواسطة شركات الائتمان لاستخدام بطاقات الائتمان في تنفيذ العمليات التجارية.

وكانت شركتا –فيزا كارد وماستركارد– قد أصدرتا تحذيرات لحاملي البطاقات، بأن الشركتين لا تضمنان ما ينتج عن المعاملات المالية عبر الإنترنت من مخاطر، الأمر الذي أدّى إلى إحجام العديد من المستخدمين عن استعمال بطاقات الائتمان، إلا أنه وبعد إقرار استخدام نظام المعاملات الإلكترونية الآمنة (SET). قامت الشركتان بإلغاء هذه التحذيرات وعاد نمو استخدام بطاقات الائتمان مرة أخرى إلى الظهور[2].

---

1 وهي اختصار لعبارة: Secure Encryption Payment Protocol ، وارد بمؤلف عبد الفتاح بيومي حجازي: التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص 276.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، مرجع سابق، ص277.

ويقال إنّ نظام المعاملات الإلكترونية الآمنة يحقّق درجة من التشفير أعلى من تلك التي تستعملها الولايات المتحدة الأمريكية ضمن الأنظمة العسكرية الخاصة به، وذلك لأنها تستخدم طبقات متعددة من التشفير يصعب فكّها[1].

ونظام المعاملات الإلكترونية الآمنة يحقّق المزايا الآتية:

التكاملية، بمعنى أنه يضمن أن الرسالة المرسلة هي ذاتها الرسالة المستقبلة، وسرية المعاملة، وذلك من خلال تشفير محتوى الرسالة والمعلومات المالية الموجودة بها، والتحقّق من شخصية البائع، وذلك من خلال شهادة التحقّق.

وعندما يرغب المشتري في نظام المعاملات الآمنة، فإنّه يتقدّم لأحد البنوك أو أحد شركات الائتمان التي توفّر خدمات نظام المعاملات الآمنة، ويحصل على زوج من مفاتيح التشفير العامة، وزوج من مفاتيح التشفير الخاصة، وشهادة رقمية للمشتري في صورة ملف معلوماتي.

ويحصل البائع المشترك في النظام ذاته، على مفاتيح التشفير ذاتها، وكذلك شهادة رقمية خاصة به في صورة ملف معلوماتي.

ويتم استخدام هذه المفاتيح فيما بينهما لأجل تشفير الرسالة المتبادلة، مع مراعاة أن الأجزاء المالية من الرسالة لها تشفير خاص ينطوي على درجة تأمين عالية، عكس البيانات الأخرى، وذلك وفق طريقة فنية معقّدة لا يشعر بها البائع أو المشتري، لأنّ متصفّح خدمة الإنترنت الخاص بهما يتولى هذه المهامّ وفق برامج معيّنة[2].

---

1 رأفت رضوان، مرجع سابق، ص 93 وما بعدها.

2 رأفت رضوان، مرجع سابق، ص 99 و100.

والملاحظ أنّ نجاح التشفير يقتصر على كون كلّ من المعلومات والمفتاح اللذين يراد تشفيرها محميّ وكشفها لمخاطر أخرى، فمثلاً وجود الفيروسات أو برامج التجسّس على جهازك سيؤدي إلى كشف كلمة المرور أو يؤدّي إلى تخريبها. وهذا يحصل عندما تكتب كلمة المرور على الجهاز من خلالها برنامج التجسس يقوم بسرقة الكلمة وكشفها أو إذا قمت بتخزين المفتاح الذي تحتاج إليه لفك التشفير في المكان نفسه الذي خزنت فيه المعلومات المشفرة، سيكون مثلما تكتب كلمات المرور المهمة على أوراق وتضعها في أماكن تسهل سرقتها.

لذا أرى أن التشفير عملية تجري موازية لها عملية أخرى وهي إمكانية الخرق وكشف المفاتيح، وهذا الصراع بدأ بين الطرفين منذ ظهورها ويستمر على هذا المنهج، على الرغم من وجود طرائق تشفير متينة وقوية لا يسهل اختراقها. مع ذلك تبقى عملية التشفير الطريق الآمن لإجراء العمليات بين الأطراف، وهو طريق متمتّع بالصفة القانونية في بيئة إلكترونية، وبوساطة تقنيات ووسائل اتصالات حديثة وتكنولوجية.

المبحث الثاني

طرق التحقّق من سلامة الرسالة والمصادقة عليها

تمهيد وتقسيم:

للتثبّت من صحة توقيع إلكتروني وسلامة الرسالة والمصادقة عليها لا بد من وجود استراتيجية مقنعة لكي يتم ربط شخص أو هيئة معيّنة بزوج المفاتيح العام والمتماثل. ولكن الحلّ في استخدام طرف ثالث واحد أو أكثر يكون موثوقًا به لكي يربط موقع معيّن مع مفتاح عام محدّد. تلك الجهة الثالثة الموثوق بها يشار إليها بعبارة "جهة التصديق الإلكتروني" يقوم بإصدار شهادة اعتماد توقيع معين لجهة معيّنة.

وللتحقّق من الرسالة والمصادقة عليها كان لا بد من وجود ما يسمّى بإجراءات التوثيق والتصديق المحكمة، وهي الإجراءات التي تهدف إلى التحقّق من أنّ الرسالة الإلكترونية قد صدرت من شخص معيّن، والكشف عن أيّ خطأ أو تعديل في محتويات أو في نقل أو تخزين رسالة إلكترونية أو سجل إلكتروني خلال فترة زمنية محددة، ويشمل ذلك أيّ إجراء يستخدم مناهج حسابية أو رموز أو كلمات أو أرقام تعريفية أو تشفير أو إجراءات للرد أو لإقرار الاستلام وغيرها من وسائل إجراءات حماية المعلومات.

وفيما يأتي سأتطرق إلى الحديث عن طرق التحقّق من سلامة الرسالة والمصادقة عليها من خلال المطلبين الآتيين:

المطلب الأول: تصديق التوقيع الإلكتروني والجهة المسؤولة عنه

المطلب الثاني: شهادة التصديق الإلكتروني

المطلب الأول: تصديق التوقيع الإلكتروني والجهة المسؤولة عنه

إنّ معظم قوانين التجارة الإلكترونية والقوانين الخاصة بالتوقيع الإلكتروني تؤكّد ضرورة شهادة صادرة عن طرف ثالث توثّق صحّة التوقيع الإلكتروني وتصادق عليه[1]، بحيث أصبح بالإمكان توفير الأمان القانوني في معاملات التجارة الإلكترونية والتوقيعات الإلكترونية، بفعل تدخّل شخص ثالث محلّ ثقة يقوم ببيان هوية الأطراف والتأكّد من صحة توقيعاتهم ونسبتها إليهم عن طريق استخدام تقنية تسمى (public keu infrastructure)، والتي تسمى اختصارًا بـــ (pki)، إذ إنّ القوة الثبوتية للتوقيع الإلكتروني تعتمد بصورة رئيسية على موثوقية النظام المعلوماتي المستخدم في المعاملات التجارية[2].

ويعتبر التوقيع الإلكتروني أحد الضمانات المهمة لأطراف المعاملة أو العقد الذي يتم بوسائل إلكترونية حيث يتيح للطرفين التحقق والتأكّد من هوية الطرف الآخر، ممّا يساعده باتخاذ قراره بالدخول بعلاقة تعاقدية مع الطرف المقابل بقناعة تامّة.

الفرع الأول: مفهوم التصديق الإلكتروني

لكي يكون التوقيع الإلكتروني ضمانة حقيقية لأطراف المعاملة الإلكترونية يجب أن يكون مصدّقًا حيث يعتبر التصديق أحد الضمانات القانونية لإثبات صحة التوقيع الإلكتروني، وبالتالي صحّة المعاملات الإلكترونية، ولم يعرف قانون المعاملات

---

1 حسون علي حسون الفتلاوي، التوقيع الإلكتروني، دراسة مقارنة، رسالة ماجستير مقدمة الى مجلس كلية القانون في جامعة بابل، 2006م، ص30.

2 باسيل يوسف، الاعتراف القانوني بالسندات والتواقيع الإلكترونية في التشريعات المقارنة، بحث منشور في مجلة دراسات قانونية، بيت الحكمة، بغداد، العدد الرابع، 2000م، ص 22.

والتجارة الإلكترونية التصديق الإلكتروني ولكنه عرّف مزوّد خدمات التصديق بأنه[1] "أيّ شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أيّة خدمات أو مهمّات متعلّقة بها وبالتواقيع الإلكترونية والمنظمة بموجب أحكام الفصل الخامس من هذا القانون". كما أشار المشرع الإماراتي إلى تعريف شهادة المصادقة الإلكترونية بأنها شهادة يصدرها مزوّد خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معيّنة، ويشار إليها في هذا القانون بـ "الشهادة"[2].

كما أشار إليها في قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية على[3] "القائم بخدمات التصديق الإلكتروني: كلّ شخص طبيعي أو اعتباري مرخّص له بإصدار شهادات التصديق الإلكتروني وفقًا للمواصفات والشروط والضوابط الدولية والمقرّرة من الجهة المختصّة، ويؤدّي خدمات أخرى ذات علاقة بالتوقيع الإلكتروني، كما يتمّ بواسطتها وضع وتثبيت التوقيع إلكترونيًا على دعامة إلكترونية"[4].

---

1 المادة (2) من قانون المعاملات والتجارة الإلكترونية التصديق الإلكتروني رقم (2) لسنة 2002 والخاص بإمارة دبي.

2 المادة (2) من قانون المعاملات والتجارة الإلكترونية رقم (2) لسنة 2002 والخاص بإمارة دبي.

3 المادة (1/ 13) من قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012م.

4 قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية قي الدول العربية رقم (101) لسنة 2012 بنص المادة (1/ 13).

وقد أوردت القوانين العربية أيضًا تعريفات مشـــابهة لمـــا ورد فـــي القـــانون النموذجي، فقد عرّف القانون المصري الموقع بأنه[1] "الشخص الحائز على بيانـــات إنشاء التوقيع ويوقع عن نفسه أو عمّن ينيبه أو يمثّله قانونًا) ثم انتقل في الفقـــرة (و) من المادة نفسها ليعرّف شهادة التصديق الإلكترونية بأنها "الشهادة التي تصـــدر مـــن الجهة المرخّص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع"[2].

كما عرف القانون الأدرني شهادة التوثيق في متنه على أنها [3] "الشـــهادة التـــي تصدر عن جهة مختصّة مرخصّة أو معتمدة لإثبات نسبة توقيـــع إلكترونـــي إلـــى شخص معيّن استنادًا إلى إجراءات توثيق معتمدة[4].

وكذلك القانون العراقي لم يعرف التصديق الإلكترونـــي إلا أنـــه عـــرف جهـــة التصديق بأنها[5] "الشخص المعنوي المرخّص له إصدار شهادات تصـــديق التوقيـــع الإلكتروني وفق أحكام هذا القانون"، كما أشار المشرع العراقي إلى تعريف شـــهادة التصديق الإلكترونية بأنها[6] "الوثيقة التي تصدرها جهة التصديق وفق أحكـــام هـــذا القانون، والتي تستخدم لإثبات صحة نسبة التوقيع الإلكتروني إلى الموقع)[7].

كما أصدر المجلس الأوروبي التوجيه الأوروبي الخاص بالتوقيعات الإلكترونية الذي يهدف إلى توحيد قوانين الدول الأعضاء في الاتحاد الأوروبي، بحيـــث يجـــب

---

1 المادة (1)/ الفقرة هاء من القانون المصري للتوقيع الإلكتروني رقم (15) لسنة 2004.

2 القانون المصري للتوقيع الإلكتروني رقم (15) لسنة 2004.

3 المادة (2) من القانون الأردني للمعاملات الإلكترونية رقم (85) لسنة 2001.

4 القانون الأردني للمعاملات الإلكترونية رقم (85) لسنة 2001.

5 المادة (1/ 15) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي.

6 المادة (1/ 12) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي.

7 جاء بالمعنى نفسه نص المادة (12/1) من قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني.

عليهم إدخال القواعد القانونية التي نصّ عليها ذلك التوجيه في قوانينها، ممّا يعني ضرورة اتخاذ الدول الأعضاء الإجراءات اللازمة لإدماج أحكام التوجيه في قوانينها الداخلية في مدة أقصاها ثمانية عشر شهرًا من تاريخ نفاذ ذلك التوجيه، وقد أوضح التوجيه الأوروبي مفهوم التوقيع الإلكتروني المصدق على أنه[1] "يجب على الدول الأعضاء أن تعمل على أن يكون التوقيع الإلكتروني المتقدّم أو المعزّز والمبني على شهادة تصديق معتمدة وتم إنشاؤه بأداة آمنة، ويعني ذلك ضرورة استناد التوقيع الإلكتروني إلى شهادة التصديق حتى يكون مصدقًا أو معزّزًا أو متقدمًا، ومن ثم فلا بد من توافر شهادة التصديق الإلكتروني لكي يكون التوقيع الإلكتروني مصدقًا، وبيّن التوجيه الأوروبي مفهوم شهادة التصديق بأنها[2] "شهادة إلكترونية تربط بين بيانات التحقّق من التوقيع وبين شخصٍ معيّنٍ، وتؤكّد هوية الموقع. ويتّضح من المادة السابقة أن الهدف الرئيسي من شهادة التصديق هو تأكيد نسبة التوقيع الإلكتروني إلى شخص معين وتعيين هويته بشكل دقيق؛ أي: تعمل تلك الشهادة على تصديق التوقيع الإلكتروني الخاص بالموقع بما يثبت هويته بصورة قاطعة، ومن هنا تظهر أهمية الحاجة إلى تصديق التوقيع الإلكتروني، لأنه دون هذا التصديق لا يتسنى للمتعاقدين عبر الإنترنت التأكّد من هوية المتعاملين معهم، بحيث قد يدّعي شخص هوية معيّنة، ومن ثم فشهادة التصديق الإلكتروني تفيد التصديق على التوقيع الإلكتروني بحيث تشهد بصحته ونسبته إلى من صدر عنه، فإذا قام أحد الأطراف بوضع توقيعه

---

1 المادة (5) من التوجيه الأوروبي رقم (93) لسنة 1999.

2 المادة (2) من التوجيه الأوروبي رقم (93) لسنة 1999.

الإلكتروني المصدق بتلك الشهادة على محرر إلكتروني، فإنّ ذلــك يعــزّز صــدور التوقيع عن صاحبه[1].

ولكي يتم ربط زوج من المفاتيح بموقع محتمل تقوم "جهة التصديق الإلكتروني" بإصدار شهادة، سجل إلكتروني يذكر فيه المفتاح الشفري العام على أنه "موضــوع" الشهادة، ويؤكد بأنّ الموقع المحتمل المعرف عنه في الشهادة يحمل المفتاح الخــاص المقابل. يشار إلى الموقع المحتمل بعبارة "المشترك". إنّ وظيفة الشهادة الرئيسية هي ربط زوج من المفاتيح مع مشترك معين؛ أي: "مستلم" للشهادة يرغب في الاعتمــاد على والوثوق بتوقيع إلكتروني ينشئه المشترك المذكور في الشهادة (عندئــذ يصــبح المستلم هو الطرف المعتمد) بإمكانه استخدام المفتاح الشفري العــام المــذكور فــي الشهادة للتثبّت من صحّة التوقيع الإلكتروني؛ أي: بأنه تم إنشاؤه بواســطة المفتــاح الخاص المقابل. وفي حال نجحت عملية التثبّت من الصحة فإنّ هذه السلســلة مــن الوقائع والمقدمات توفر الثقة والضمان بأنّ المفتاح الخاص المقابل محتفظ به من قبل المشترك المذكور اسمه في الشهادة، وبأن التوقيع الإلكتروني قد تم إنشاؤه من قبــل ذلك المشترك[2].

يتبيّن لنا من خلال ما تقدم أنّ التصديق الإلكتروني عبارة عن وسيلة فنية وتقنية آمنه تستخدم للتأكد من صحة صدور التوقيع الإلكتروني أو المحرر الإلكتروني مــن خلال نسبته إلى شخص معيّن من قبل جهة محايدة يطلق عليها جهــة التصــديق أو القائم بخدمات التصديق وتقوم الجهة الأخيرة من خلال إصدارها لشــهادة التصــديق

---

1 إيناس الخالدي، مرجع سابق، ص38-39.

2 عبد الرسول عبد الرضا، محمد جعفر هادي، مرجع سابق، ص 17.

الإلكترونية بعملية التصديق، والتأكّد من صحة التوقيع الإلكتروني وربطة بالبيانات الواردة بالسند الإلكتروني .

الفرع الثاني: الجهة المسؤولة عن التصديق

إنّ عاملي الثقة والأمان يأتيان في مقدمة الضمانات التي يبحث عنها المتعاملون والتي يتوجّب توافرها لازدهار المعاملات الإلكترونية وتطورها، ومن المعروف لدينا أنّ هذه المعاملات تتم بين أشخاص متباعدين مكانيًّا، وفي الغالب لا يعرف بعضهم البعض الآخر، وهذا الأمر يستوجب توفير الضمانات والآليات التقنية الكفيلة بتحديد هوية الأطراف وتحديد حقيقة التعامل ومضمونه، وفي هذه الحالة يتوجّب أن يكون هناك طرف ثالث ومحايد موثوق به يقوم بالتأكد من صحة صدور الإرادة التعاقدية من الطرف الآخر، والتأكّد من جدّيّة هذه الإرادة وبعدها عن الغش والاحتيال، بالإضافة إلى تحديد مضمون الإرادة تحديدًا دقيقًا يمكّن المتعامل من الاعتماد عليه في تعامله وربط المتعامل الآخر (سواء كان شخصًا طبيعيًّا أم معنويًّا) بالتوقيع العائد له(1).

وقد تنوّعت التسميات المطلقة على الجهة المختصّة بتصديق التوقيع الإلكتروني من جهة التصديق إلى مقدم أو مزود خدمات التصديق إلى سلطة المصادقة على التوقيع الإلكتروني، ويرى البعض إن تسمية الكاتب العدل الإلكتروني هي التسمية الجديرة بالاعتماد منطلقًا بذلك من أنّ وظيفة الكاتب العدل الإلكتروني بوصفة جهة تقنية حيادية، وتصديقه للسندات الكتابية الاعتيادية سواء ما يتعلق بإجراءات التوثيق

---

1 عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنت، دار الكتب القانونية، مصر، 2008م، ص 102.

أم الضمان، إذ تكاد تكون مساوية لضمانات الكاتب العدل لا سيما فيما يتعلّق باحتفاظ الكاتب العدل الإلكتروني بنسخة من السندات الإلكترونية وهويات أصحابها وبصماتهم الإلكترونية[1].

ويقصد بجهات التوثيق والتصديق الإلكتروني الشخص المسؤول عن إصدار شهادة تتضمّن تحديد هوية الموقع وتثبيت صلته بالتوقيع الإلكتروني، فهو يؤثر تأثيرًا أساسيًّا في مجال المعاملات القانونية الإلكترونية، إذ يعدّ بمثابة حلقة الوصل بين المرسل والمرسل إليه اللذان لا يعرف- عادة- أحدهما الآخر، ولولا وجود هذا الشخص لأحجم الكثير من المتعاملين عن الإقدام على التعامل القانوني الإلكتروني[2].

إنّ القانون الإماراتي عرّف جهة التصديق الإلكتروني بمصطلح مزود خدمات التصديق بأنه[3] (أيّ شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أية خدمات أو مهمّات متعلّقة بها وبالتوقيعات الإلكترونية والمنظمة بموجب أحكام هذا القانون)[4].

---

1 عباس العبودي، مرجع سابق، ص 196.

2 أيمن سعد سليم، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2004م، ص 83.

3 المادة (1) في كل من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية وقانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية والخاص بإمارة دبي

4 المادة (1) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية.

هذا ويعيّن بقرار من مجلس الوزراء الإماراتي جهة لمراقبة خدمات التصديق، وعلى وجه الخصوص لأغراض ترخيص وتصديق ومراقبة أنشطة مزوّدي خدمات التصديق والإشراف عليها[1].

أمّا بالنسبة للمشرع المصري لم يعرف جهة التصديق الإلكتروني ضمن قانون التوقيع الإلكتروني المصري لكن عاد وأعطى تعريفًا لجهة التصديق الإلكترونية بأنها[2] "الجهات المرخّص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلّق بالتوقيع الإلكتروني".

وقد عرّف القانون التونسي مزوّد خدمات التصديق بأنه[3] "كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرّف في شهادات المصادقة ويبدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني"[4].

أمّا الموقف في القانون الفرنسي فنلاحظ إنّ المشرع عرف جهة التصديق الإلكتروني بمقدم خدمة التصديق بأنه "أيّ شخص يقدّم شهادات التصديق أو خدمات أخرى في مجال التوقيع الإلكتروني"[5] .

---

1 المادة (20) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية.

2 البند (6) من المادة (1) من قرار وزير الاتصالات وتكنولوجيا المعلومات رقم (109) لسنة 2005.

3 قانون المبادلات والتجارة الإلكترونية التونسي رقم (83) لسنة 2000.

4 المادة الفصل (2) من قانون المبادلات والتجارة الإلكترونية التونسي رقم (83) لسنة 2000.

5 المادة (1/ 11) من المرسوم رقم (272) لسنة 2001.

وعرّف قانون الأونيسترال النموذجي للتوقيعات الإلكترونية لسنة 2001م مقدم خدمات التصديق بأنه "شخص يصدر الشهادات، ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية"[1].

أوّلاً: واجبات مزود خدمات التصديق

اشترط المشرع الإماراتي بأنه يجب على مزوّد خدمات التصديق أن يتصرف وفقاً للبيانات التي يقدّمها بشأن ممارسته لنشاطه، وأن يمارس عناية معقولة لضمان دقة واكتمال كلّ ما يقدّمه من بيانات جوهرية ذات صلة بشهادة المصادقة الإلكترونية أو مدرجة فيها طيلة سريانها، وأن يوفّر وسائل يكون من المعقول الوصول إليها وتمكن الطرف الذي يعتمد على خدماته من التأكّد من هوية مزود خدمات التصديق، وأن الشخص المعينة هويته في شهادة المصادقة الإلكترونية، لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في هذه الشهادة، والطريقة المستخدمة في تعيين هوية الموقع، ووجود أيّة قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع، وما إذا كانت أداة التوقيع صحيحة ولم تتعرض لما يثير الشبهة، وما إذا كان للموقع وسيلة لإعطاء إخطار بموجب هذا القانون، وما إذا كان هناك وسيلة مناسبة للإبلاغ عن إلغاء التوقيع.

وأن يوفر وسيلة للموقعين تمكّنهم من تقديم إخطار بأن أداة التوقيع قد تعرّضت لما يثير الشبهة، وأن يضمن توافر خدمة إلغاء للتوقيع يمكن استخدامها في الوقت

---

1 المادة (2/هـ) من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.

المناسب، وأن يستخدم في أداء خدماته نظامًا وإجراءات وموارد بشرية جديرة بالثقة، وأن يكون مرخصًا من مراقب خدمات التصديق إذا كان يعمل في الدولة[1].

ولتقرير ما إذا كانت أيّة نظم أو إجراءات أو موارد بشرية جديرة بالثقة يتعيّن الأخذ في الاعتبار بأن الموارد المالية والبشرية بما في ذلك توافر الموجودات داخل منطقة الاختصاص، ومدى الثقة في برامج وأجهزة الحاسب الآلي، وكذلك إجراءات معالجة وإصدار شهادات المصادقة الإلكترونية، وطلبات الحصول على هذه الشهادات والاحتفاظ بالسجلات، وتوفير المعلومات الخاصة بالموقّعين المحدّدين في شهادات المصادقة الإلكترونية، وكذلك توفير المعلومات للأطراف المعتمدة على خدمات التصديق، ومراجعة الحسابات من جانب جهة مستقلّة، ووجود إعلان من الدولة أو من جهة اعتماد، أو من مزوّد خدمات التصديق بشأن وجود ما ذكره أو الالتزام به، وخضوع مزود خدمات التصديق للاختصاص القضائي لمحاكم الدولة، ومراعاة مدى التناقض بين القانون المطبّق على أعمال مزوّد خدمات التصديق وقوانين الدولة.

ويجب أن تحدّد شهادة المصادقة الإلكترونية هوية مزوّد خدمات التصديق، وأن الشخص المعيّنة هويته في شهادة المصادقة الإلكترونية لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في هذه الشهادة، وأن أداة التوقيع كانت سارية المفعول في أو قبل تاريخ إصدار شهادة المصادقة الإلكترونية، وما إذا كانت هناك أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع أو

---

1 المادة (21) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية الإماراتي.

شهادة المصادقة الإلكترونية، وما إذا كانت هناك أية قيود على نطاق أو مدى المسؤولية التي قبلها مزوّد خدمات التصديق اتجاه أيّ شخص[1].

وإذا حدثت أيّة أضرار نتيجة لعدم صحة شهادة المصادقة الإلكترونية أو نتيجة لأيّ عيب فيها، يكون مزوّد خدمات التصديق مسؤولاً عن الخسائر التي يتكبّدها كلّ طرف تعاقد مع مزوّد خدمات التصديق حول تقديم شهادة المصادقة الإلكترونية، وأيّ شخص اعتمد بصورة معقولة على شهادة المصادقة الإلكترونية التي أصدرها مزوّد خدمات التصديق.

ولا يكون مزوّد خدمات التصديق مسؤولاً عن أيّ ضرر إذا أدرج في شهادة المصادقة الإلكترونية بيانًا يقيد نطاق ومدى مسؤوليته اتجاه أيّ شخص ذي صلة، وفقًا للائحة التي تصدر في هذا الشأن، وإذا أثبت أنه لم يرتكب أيّ خطأ أو إهمال، أو أن الضرر قد نشأ عن سبب أجنبي لا يد له فيه.

ثانيًا: مسؤولية مزوّد خدمات التصديق

أمّا المهام التي تقوم بها جهات التصديق فقد حددها المشرع الإماراتي "حيث يصدر الوزير بناءً على اقتراح المراقب اللوائح الخاصة بتنظيم وترخيص عمل مزودي خدمات التصديق الذين يعملون في الدولة، بما في ذلك ترخيص وتجديد ترخيص مزوّدي خدمات التصديق وممثّليهم المفوّضين، وتجديد هذه التراخيص والمسائل المتعلّقة بها، وأنشطة مزوّدي خدمات التصديق، ويشمل ذلك طريقة ومكان وأسلوب الحصول على أعمالهم وجذب الجمهور لها، والمعايير والقواعد التي يتعيّن

---

1 المادة (21) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية الإماراتي.

على مزودي خدمات التصديق المحافظة عليها واتباعها في أعمالهم، وتحديد المعايير المناسبة فيما يتعلّق بمؤهلات وخبرة مزودي خدمات التصديق وتـدريب مـوظّفيهم، وتحديد شروط إدارة الأعمال التي يقوم بهـا مـزوّد خـدمات التصـديق، وتحديـد محتويات وتوزيع المواد والإعلانات المكتوبة أو المطبوعة أو المرئية، والتي يجـوز أن يوزعها أو يستخدمها أيّ شخص فيما يتعلّق بأية شهادة مصـادقة إلكترونيـة أو مفتاح رقمي، وتحديد شكل ومحتوى أية شهادة مصادقة إلكترونية أو مفتاح رقمي[1].

وكذلك تحديد التفاصيل التي يجب تدوينها في الحسابات التي يحتفظ بهـا مـزود خدمات التصديق، والمؤهلات الواجب توافرها في مدققي حسابات مزودي خـدمات التصديق، ووضع القواعد اللازمة لتنظيم التفتيش والتدقيق على أعمال مزود خدمات التصديق، وشروط إنشاء وتنظيم أيّ نظام إلكتروني بواسطة مزود خدمات التصديق، سواء بمفرده أو بالاشتراك مع مزوّدي خدمات تصديق آخرين، وفرض وتغيير تلـك الشروط أو القيود وفقًا لاقتراح المراقب وبالتنسيق مع الجهـات ذات الاختصـاص، والطريقة التي يدير بها الحاصل على الترخيص معاملاته مع عملائه، وكذلك عنـد تعارض مصالحه مع مصالحهم، وواجباته اتجاههم فيما يتصل بشهادات المصـادقة الإلكترونية الرقمية، واقتراح الرسوم التي يجب استيفاؤها فيما يتصـل بـأيّ أمـر مطلوب بموجب أحكام هذه المادة، ويصدر بهذه الرسوم قرار من مجلس الـوزراء، ووضع أية نماذج لأغراض تطبيق هذه المادة، والغرامات المالية والجزاءات المقررة على مخالفة قواعد ترخي وتنظيم عمل مزودي خدمات التصديق[2].

---

1 المادة (22) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية.
2 المادة (22) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية.

أمّا بالنسبة للمشرع العراقي فإنه ولكي تتمكّن جهة التصديق الإلكتروني من مزاولة عملها فإنّ عليها الحصول على ترخيص من الجهة التي حدّدها القانون، وفقًا لقانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي فإنّ الجهة التي تمنح الترخيص تتمثّل بالشركة العامة لخدمات الشبكة الدولية للمعلومات في وزارة الاتصالات، وقد حدّد القانون واجبات هذه الشركة في متن القانون أعلاه والتي نصت على[1] "أن تتولى الشركة منح تراخيص إصدار شهادات التصديق بعد استحصال موافقة الوزير وفقًا للقانون، وتحديد المعايير الفنية لأنظمة التوقيع الإلكتروني وضبط مواصفاتها الفنية والتقنية، والمتابعة والإشراف على أداء الجهات العامة في مجال إصدار شهادات التصديق وتقييم أدائها، والنظر في الشكاوى المتعلقة بأنشطة التوقيع الإلكتروني أو تصديق الشهادة والمعاملات الإلكترونية واتخاذ القرارات المناسبة في شأنها وفقًا للقانون، وتقديم المشورة الفنية للجهات العاملة في مجالات التوقيع الإلكتروني وتصديق الشهادات، وإقامة الدورات التدريبية للعاملين في مجالات التوقيع الإلكتروني وتصديق الشهادات إقامة الندوات والمؤتمرات التثقيفية بهذا الخصوص"[2].

وقد اشترط المشرع العراقي على الشركة عند مزاولتها لنشاط منح الترخيص عبر إصدار شهادة التصديق عدة شروط "تراعي الشركة عند منح الترخيص بمزاولة نشاط إصدار شهادة التصديق، وضمان المنافسة والعلانية في اختيار المرخص له،

---

1 المادة (6) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي.

2 مجلة المحقّق الحلي للعلوم القانونية والسياسية، العدد الثالث، السنة السابعة 2015م، ص 85-86.

وتحديد مدة مناسبة لنفاذ الترخيص، وتحديد وسائل الإشراف والمتابعة الفنية والمالية بالشكل الذي يضمن حسن أداء الجهات المرخّص لها، وعدم جواز التوقّف عن مزاولة النشاط المرخّص به أو الاندماج مع جهات أخرى أو التنازل الكلّيّ أو الجزئيّ عن الترخيص للغير خلال مدة نفاذيته إلا بعد الحصول على موافقة الشركة ووفقًا للقانون، وأن تكون للمرخص له المستلزمات البشرية والمادية اللازمة لممارسة مهنة تصديق التواقيع الإلكترونية، وأن يقدّم كفالة ضامنة للوفاء بالغرامات أو التعويضات أو الالتزامات المالية الأخرى على أن تبقى الكفالة قائمة طيلة مدة الترخيص، وأن يكون له موقع عمل ثابت ومعلوم لممارسة النشاط المتّصل بالترخيص، وتأييد الجهات المختصّة بعدم وجود مانع أمني يحول دون منح الترخيص"[1].

أمّا المهام التي تقوم بها جهات التصديق فقد حدّدها المشرع العراقي[2]، والتي تتمثّل بإصدار وتسلم وحفظ شهادات التصديق الإلكتروني، وذلك خلال استعمال آليات وبرامج موثوق بها في سبيل حمايتها من التقليد والاحتيال[3].

والغرض من إصدار مثل هذه الشهادات هو الاعتراف بوجود صلة ما بين الموقع وبيانات إنشاء التوقيع الإلكتروني أو التأكّد من هوية وشخصية مستخدم

---

1 المادة (8) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي.

2 المادة (10/ أولاً، ثانيًا، ثالثًا) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية.

3 المادة (10/ أولاً) تنص على ((إصدار وتسلم وحفظ شهادات التصديق الإلكتروني باستعمال آليات وبرامج موثوق من أجل حمايتها من التقليد والاحتيال)). كما نصّت المادة (8) من قانون تصديق اتفاقية تنظيم أحاكم التوقيع الإلكتروني على أنه ((يتولى بخدمات التصديق الإلكتروني إصدار وتسلم وحفظ شهادات التصديق الإلكتروني وفقًا للشروط والضوابط التي تحدّدها الجهة المختصّة)).

التوقيع الإلكتروني، كما فرض القانون على جهة التصديق أن تقوم بتنظيم سجل إلكتروني تدوّن فيه شهادات التصديق الإلكتروني، وكلّ المعلومات التي تخصّها، وتلتزم جهة التصديق بإتاحة الاطلاع على هذا السجل من كلّ تغيير غير مشروع[1].

بالإضافة إلى ذلك، تقوم جهة التصديق بضمان صحة المعلومات الواردة في شهادة التصديق الإلكترونية، كما تضمن الصلة ما بين الموقع ومنظومة التدقيق والمراجعة الخاصة بتوقيعه[2].

ثالثًا: الرقابة على مزوّد خدمات التصديق

أمّا الالتزامات التي تقع على عاتق جهة التصديق الإلكترونية فقد حدّدها المشرع العراقي بصورة واضحة ضمن قانون التوقيع الإلكتروني والمعاملات الإلكترونية، وتتمثّل في الالتزام بتعليق العمل بشهادة التصديق فورًا في حالة إذا ما طلب الموقع ذلك[3].

وكذلك تلتزم جهة التصديق بإلغاء شهادة التصديق الإلكترونية فورًا في حالة إذا ما أعلم بوفاة الموقع إذا كان شخصًا اعتباريًّا، كذلك إذا توصل بعد تدقيقه للمعلومات

---

1 المادة (10/ ثانيًا) تنصّ على ((مسك سجل إلكتروني لشهادات التصديق مفتوح للاطلاع عليه إلكترونيًّا باستمرار من المتعاملين مع الموقعين على المعلومات ذات العلاقة بما فيها تاريخ تعليق الشهادات أو إلغائها على أن يلتزم بحمايته من كلّ تغيير غير مشروع)).

- كما جاءت بالمعنى نفسه المادة (15) من قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني.

2 المادة (10/ ثالثًا) تنصّ على ((ضمان صحة المعلومات المصادق عليها في الشهادة في تاريخ تسلمها والصلة ما بين الموقع ومنظومة التدقيق والمراجعة الخاصة بتوقيعه وانفراد الموقع بمسك منظومة إنشاء توقيعه الإلكتروني)) .

- كما جاءت بالمعنى نفسه المادة (10) من قانون تصديق اتفاقية تنظيم أحاكم التوقيع الإلكتروني.

3 المادة (11/ أولاً) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي.

إنها خاطئة أو مزيّفة أو إنها غير مطابقة للواقع أو أنه قد تم انتهاك منظومة إنشـــاء التوقيع الإلكتروني أو تم استعمال شهادة التصديق استعمالاً مدلسًا أو غير مشروع[1].

كذلك تلتزم جهة التصديق والعاملين فيها ممّن يتاح لهم الاطلاع على المعلومات والبيانات الخاصة بالتوقيع الإلكتروني والوسائل الإلكترونية الحفاظ علـــى ســـريتها وعدم إفشائها للغير أو استخدامها في غير الغرض الذي قدّمت من أجله[2].

وفي الوقت نفسه ألزم المشرع جهة التصديق بتقديم ما تطلبه المحكمة أو الشركة من تقارير ومعلومات تتعلّق بالنشاطات التي تزاولها[3].

أمّا عن موقف المشرع المصري فنلاحظ أنه أناط مهمّة منح إصـــدار شـــهادات التصديق الإلكتروني إلى هيئـــة تنميـــة صـــناعة تكنولوجيـــا المعلومـــات، وحـــدّد اختصاصاتها، وذلك ضمن المادة (4) من قانون التوقيع الإلكتروني المصري[4].

ولم يذكر المشرع المصري المهام التي تقوم بها جهات التصـــديق الإلكترونـــي ضمن قانون التوقيع الإلكتروني أو لائحته التنفيذية، وإنما ترك تحديدها إلـــى هيئـــة

---

1 المادة (14) من قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012.

2 المادة (12/ ثانيًا) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية.

3 المادة (18) من قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012م، والتي نصّت على أنه ((تعتبر بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى القائم بخدمات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت آلية أو اتصل بها بحكم عملة إفشاء أيّ من هذه البيانات للغير أو استعمالها في غير الغرض الذي قدمت من أجله)).

4 المادة (18) من قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012م.

صناعة تكنولوجيا المعلومات، والتي أوردتها ضمن الترخيص الصادر منها رقم (103) لسنة 2006م، والذي تم بموجبة منح التراخيص لجهات التصديق الإلكتروني لمزاولة أعمالها بتقديم خدمات التوقيع الإلكتروني، حيث حدّدت المادة (45) من الترخيص مجموعة من الخدمات يجب على جهة التصديق القيام بتقديمها ولا يجوز لها أن تقدّم أيّة خدمات أخرى دون الحصول على موافقة خطية مسبقة من الهيئة، وهذه الخدمات تتمثّل بتسجيل وإصدار شهادات التصديق الإلكتروني، وإصدار أدوات إنشاء التوقيع الإلكتروني وتثبيته[1].

إنّ هيئة صناعة تكنولوجيا المعلومات المصرية فرضت على عاتق جهة التصديق خدمة إصدار أدوات إنشاء وتثبيت التوقيع الإلكتروني، وتتم هذه الخدمة من خلال إصدار البطاقة الذكية والجهاز القارئ لها، وقد عرفت المادة (1/ 15) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري البطاقة الذكية بأنها "وسيط إلكتروني مؤمن يستخدم في عملية إنشاء وتثبيت التوقيع الإلكتروني على المحرر الإلكتروني، ويحتوي على شريحة إلكترونية بها معالج إلكتروني وعناصر تخزين وبرمجيات للتشغيل، ويشمل الكروت الذكية والشرائح الإلكترونية المنفصلة أو ما يماثلها في تحقيق الوظائف المطلوبة بالمعايير التقنية والفنية المحددة في هذه اللائحة"[2].

إنّ هيئة صناعة تكنولوجيا المعلومات المصرية أضافت التزامًا آخر تلتزم به جهة التصديق ومضمونه قيام الأخيرة بحفظ مفتاح الشفرة الخاص بالمستخدم بطريقة

1 مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثالث، السنة السابعة 2015م، ص 87.
2 المادة (1/ 15) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

لا تسمح بفكّ شفرة المفتاح وعدم إفشاء أيّ معلومات تؤدّي إلى التوصّل إلى مفتاح الشفرة الخاصة.

أمّا بالنسبة لموقف المشرع الفرنسي فإنه اعتمد المبدأ الذي جاء به التوجه الأوروبي رقم (93) لسنة 1999 الخاص بالتوقيعات الإلكترونية ضمن المادة (2/3)، والذي ألزم الدول الأعضاء بعدم فرض أيّ قيود على إنشاء سلطات التصديق أو تطلب أيّ ترخيص مسبق، ووفقًا لهذا المبدأ تكون هناك حرية في ممارسة نشاط إصدار شهادات التصديق الإلكتروني حيث يحقّ لأيّ هيئة أن تمارس هذا النشاط دون حاجة للحصول على ترخيص مسبق من السلطات الفرنسية، وضمّن المشرع الفرنسي هذا المبدأ في المرسوم رقم (272) لسنة 2001م، وفي مقابل ذلك سمح التوجه الأوروبي أعلاه للدول الأعضاء إنشاء أنظمة الاعتماد وجهات التصديق الإلكترونية، وبالفعل أنشأ المشرع الفرنسي نظامًا لاعتماد جهات التصديق لكن هذا النظام طوعي؛ أي: يحقّ لجهة التصديق الإلكتروني أن تمارس عملها دون حاجة للحصول على اعتماد من قبل الجهة التي أنشأتها الدولة، ومقابل ذلك لها الحق في تقديم طلب لاعتمادها بشرط أن تتوافر فيها الشروط التي ينص عليها القانون، لكن يلاحظ أنّ الواقع العملي يجبر جهات التصديق على تقديم طلب لاعتمادها، والسبب في ذلك هو أنّ القانون الفرنسي اشترط لكي يتمتع التوقيع الإلكتروني بالحجية أن يتم التأكّد من صحته بمقتضى شهادة التصديق الإلكتروني المعتمدة؛ (أي: صادرة من جهة معتمدة)، وبالتالي فإنّ القانون الفرنسي ربط حجية التوقيع الإلكتروني باعتماد جهة التصديق[1].

يتّضح من خلال ما سبق أنّ نظام التوثيق أو التصديق ضروري من أجل تحديد مصدر التوقيعات وسلامتها، فالتوثيق يتطلّب التأكّد أو التحقّق من صحة ما هو مدون

---

1 سامح عبد الواحد التهامي، التعاقد عبر الإنترنت، دار الكتب القانونية، مصر، 2008م، ص 416– 417.

في البلاغ الإلكتروني، والتأكّد من الموقع على الوثيقة الإلكترونية، وأنّ التوقيع لم يتعرّض إلى عبث أو تلاعب، من هنا تظهر أهمية تحديد هوية الموقع، والتأكّد من سلامة الوثيقة، أو مضمونها التي تؤدّي في النهاية إلى الاعتراف بأهمية التوثيق من الطرف الثالث لضمان الثقة بالتوقيع الإلكتروني.

المطلب الثاني: شهادة التصديق الإلكتروني

البيانات التي يتمّ تبادلها خلال التعامل عبر شبكة الإنترنت ولخطورة وأهمية الصفقات التي تبرم فيما بين المتعاملين نجدهم يبحثون عن نظام أو وسيلة تؤمن لهم معاملاتهم وتزيل كافة مخاوفهم التي تتمثل بإمكانية الغير من الاطلاع على محتويات الرسائل المتبادلة، كما يبحثون عن وسيلة تؤكّد لهم هوية الطرف الآخر وصحة توقيعه، وهذا ما توفّره لهم جهة توثيق التوقيع الإلكتروني من خلال إصدار شهادات التوثيق الإلكتروني، وسوف أتناول في هذا المطلب التعريف بشهادة التصديق الإلكتروني في الفرع الأول ثم بيانات شهادة التوثيق في الفرع الثاني.

الفرع الأول: التعريف بشهادة التصديق الإلكتروني

عرّف المشرع الإماراتي شهادة التصديق الإلكتروني بأنها "الشهادة التي يصدرها مزوّد خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة"[1].

1 المادة (2) من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية.

وكذلك عرّفها قانون التجارة الإلكترونية بإمارة دبي بأنها "شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة علـــى أداة توقيـــع معينة، ويشار إليها في هذا القانون بالشهادة"[1].

وبالنسبة لموقف المشرع المصري فقد عرّف شهادة التصديق الإلكترونية بأنها[2] "الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقـــع وبيانات إنشاء التوقيع"[3].

ويلاحظ على تعريف المشرع المصري لشهادة التصديق الإلكتروني أنه اكتفـــى بتحديد الهدف من إصدار شهادة التصديق الإلكتروني، والذي يتمثّل بتأكيد الارتبـــاط بين التوقيع وبين بيانات إنشاء التوقيع الإلكتروني، والذي يؤدّي بـــدوره إلـــى بيـــان شخصية الموقع وهويته، والسبب في ذلك ذكرنا سابقًا أنّ جهة التصديق في فرنسا قد تكون معتمدة وقد تكون بسيطة، وفي هذه الحالة سوف يكون لدينا نوعين من شـــهادة التصديق شهادة تصديق إلكترونية معتمدة وشهادة تصديق إلكترونية بســيطة، وهـــذا على خلاف ما هو موجود في القانونين العراقي والمصري، حيث إنّ شهادة التصديق واحدة متمثّلة بشهادة التصديق التي تصدر من جهة التصديق المعتمدة.

وعرّفها المشرع العراقي بأنها[4] "الوثيقة التي تصدرها جهـــة التصـــديق وفـــق أحكام هذا القانون، والتي تستخدم لإثبات نسبة التوقيع الإلكتروني إلى الموقع".

---

1 المادة (2) من قانون التجارة الإلكترونية لإمارة دبي رقم (2) لسنة 2002.

2 المادة (1/ و) من قانون التوقيع الإلكتروني المصري والمادة (1/ 7) من اللائحة التنفيذية.

3 المادة (1/ 7) من قانون تنظيم التوقيعات الإلكترونية المصري.

4 المادة (1/ ثاني عشر) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية.

كما أورد تعريفًا لها بأنها[1] "والتي تضمنت التعريف الذي جاء به قانون التوقيع الإلكتروني مضافاً إليه عبارة ((وتشهد على صحة البيانات التي تتضمّنها))".

وعرفت الشهادة الإلكترونية في القانون التونسي بأنها "الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها، والذي يشهد من خلالها، أثر المعاينة على صحة البيانات التي تتضمنها[2].

وفي التشريع الفرنسي فقد أصدر مجلس الدولة الفرنسي مرسومًا في 2011/03/30م نصّ فيه على نموذجين من شهادات التصديق على التوقيع الإلكتروني، الأول وهو ما يمكن أن نسمّيه (النموذج المختصر)، وهذا النموذج يحتوي بيانات مختصرة عن صاحب التوقيع الإلكتروني. أمّا النموذج الآخر فيمكن أن نطلق عليه اسم (النموذج الشامل أو المطول)، وهو يحتوي على بيانات ومعلومات أكثر وأوسع نطاقًا من النموذج المختصر[3].

وشهادة التصديق هي ((مستند إلكتروني يربط بين بيانات التحقّق من التوقيع الإلكتروني وبين الموقع))[4].

---

1 المادة (1/ 12) قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية.

2 الفصل الثاني من قانون المبادلات والتجارة الإلكترونية التونسي رقم (83) لسنة 2000.

3 محمد أمين الرمي، مرجع سابق، ص 44.

4 المادة (1-9) من المرسوم رقم (272) لسنة 2001.

((9. Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;))

وجاء في قانون الأونستيرال النموذجي بشأن التوقيعات الإلكترونية شهادة التوثيق بأنها "تعني رسالة بيانات أو سجلاً آخر يؤكّد الارتباط بين الموقع وبيانات إنشاء التوقيع"[1].

وذكر التوجيه الأوروبي بأنها "تلك التي تربط بين أداة التوقيع وبين شخص معيّن، وتؤكّد شخصية الموقع من خلال استيفاء الشروط الواردة بالملحق رقم (2)"[2].

فالغرض من شهادة التوثيق الإلكترونية تأكيد صدور التوقيع الإلكتروني أو الرسالة الإلكترونية ممّن نسبت إليه، وأن توقيعه صحيح، ويؤكّد أيضًا سلامة البيانات الموقّعة من العبث، والتبديل والتلاعب والتغيير، وبذلك تكون البيانات موثقة[3].

ونظرًا لأهمية شهادة التوثيق الإلكترونية والاعتماد عليها بشكل آمن وموثوق فإنه يجب أن تصدر بطريقة تقنية موثوق بها، ومؤمنة ضدّ أيّ استعمال غير مرخص له، ويقدم مستوى عاليًا من السلامة والأمان، ويجب أن تستجيب شهادة التوثيق الإلكتروني لمقتضيات السلامة والوثوق بها[4]. وذلك باستخدام أنظمة معلوماتية متطورة تحقّق الأمان، ويعتدّ بهذه الشهادة في التعاملات الإلكترونية، ويجب على مصدر الشهادات أن يوفر وسائل يمكن الوصول إليها، وتمكّن الطرف

---

1 المادة (2/ ب) من قانون أونسيترال النموذجي بشأن التوقيعات الإلكترونية.

2 المادة الثالثة من التوجيه الأوروبي رقم (93) لسنة 1999م.

3 إبراهيم الدسرقي أبو الليل، مرجع سابق، ص 184.

4 المادة (17) من قانون المبادلات والتجارة الإلكترونية التونسي رقم (83) لسنة 2000.

الذي يعتمد على خدماته من التأكد من[1] هوية مزود خدمات التصديق والدولة التي أنشئ فيها لممارسة اختصاصاته، واسم الموقع الفعلي أو أية مزيّة خاصّة بالموقع، والطريقة المستخدمة في تعيين هوية الموقع، وتحديد بدء صلاحية الشهادة وتاريخ انتهائها ورقم تسلسلها، ووجود أيّة قيود على رقابته. والقيمة التي يجوز أن تستخدم من أجلها أداة التوقيع، والمفتاح العام الذي يمكن الوصول من خلاله إلى المفتاح الخاص للموقع الخاضع لرقابته، وما إذا كانت أداة التوقيع صحيحة، ولم تتعرّض لما يثير الشبهة، وحدود استخدام الشهادة وتحديد قيمة الصفقات التي يمكن استخدامها بشأنها، والتوقيع الإلكتروني لمقدم خدمات التصديق الذي يزوّد هذه الشهادة، وما إذا كانت هناك وسيلة مناسبة للإبلاغ عن إلغاء الشهادة، وعلى مزود خدمات التصديق أن يستخدم في أداء خدماته نظمًا وإجراءات وموارد بشرية جديرة بالثقة.

ولقد عرف جانب من الفقه شهادة التصديق الإلكتروني بأنها "شهادة تصدرها جهة وسيطة، أو جهة ثالثة ما بين طرفين متعاملين إلكترونيًّا، وتقرّر بأنّ شهادة التوثيق الإلكترونية هي توفير أمان يفيد صحة المعاملة الإلكترونية وضمانها من حيث صحة معلومات محتوى المعاملة، وصحة توقيعاتها الإلكترونية، وكذلك أطرافها"[2].

1 المادة (24-1-ج) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي، الفقرة (هـ) من المادة نفسها، الفقرات (ج، د، هـ، و) من المادة التاسعة من قانون أونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001.

2 عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، المجلد الثاني، مرجع سابق، ص 161.

أو هي[1] "وثيقة إلكترونية يصدرها الكاتب العدل الإلكتروني لإثبات صحة أو نسبة السندات الإلكترونية للأشخاص الذين صدرت منهم، وذلك طبقًا لإجراءات التوثيق المعتمدة".

كما عرفها البعض الآخر بأنها "صكّ أمان صادر عن جهة مختصّة يفيد صحة وضمان المعاملة الإلكترونية، وذلك من حيث صحة البيانات ومضمون المعاملة وأطرافها"[2].

ومن التعريفات الأخرى التي أوردها الفقه بشأن شهادة التصديق الإلكتروني بأنها "مستند إلكتروني يربط المفتاح العام وشخصًا معيّنًا ويحدّد هوية ذلك الشخص"[3].

كما عرفها البعض الآخر بأنها "الشهادة التي تصدرها جهات التوثيق المرخّص لها من قبل الجهات المسؤولة في الدولة لتشهد بأن التوقيع الإلكتروني هو توقيع صحيح ينسب إلى من أصدره، ويستوفي الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يعول عليه"[4].

1 عباس العبودي، مرجع سابق، ص 218.

2 عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، مرجع سابق، ص 454.

3 سامح عبد الواحد التهامي، مرجع سابق، ص 777.

4 إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، الكويت، 2003م، ص 83.

وهكذا فإنّ الشهادة الإلكترونية التي تصدر عن الطرف الثالث كمزود أو مجهز خدمات التصديق تسمى بشهادة المصادقة الإلكترونية[1] أو شهادة التوثيق[2]، وتتضمّن هذه الشهادة عادة توثيقًا وتصديقًا لمعلومات عن هوية كل طرف وشخصيته وسلطاته وأهليته، وتعدّ مصادقةً على صحة توقيعه الإلكتروني[3].

يتبيّن لنا من هذه التعريفات أنّ شهادة التصديق الإلكتروني عبارة عن هوية شخصية تعرف عن صاحبها، ولا بد أن تكون شهادة التصديق صادرة من جهة مختصّة ومحايدة.

إنّ الهدف من شهادة التصديق تأكيد صحة وقانونية البيانات الواردة في الشهادة، كما تؤكّد لنا صحة وقانونية التوقيع الإلكتروني.

الفرع الثاني: البيانات التي يجب توافرها في شهادة التصديق الإلكتروني

بالعودة إلى قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية، لا نجد أيّ إشارة إلى البيانات التي يجب توافرها في شهادة التصديق الإلكترونية، وبما أنّ الموضوع حديث ولم نجد له تطبيقًا في الإمارات إلى الآن إلا فيما يخصّ البيانات التي تتعلّق بشهادة التصديق،

---

1 هكذا أسماها قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم (2) لسنة 2002 في المادة الثانية منه، وكذلك القانون المصري رقم (15) لسنة 2004 في المادة الأولى منه، وكذلك قانون المبادلات والتجارة الإلكترونية التونسي رقم (83) لسنة 2000 في الفصل الثالث منه.

2 هكذا أسماها قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001 في المادة الثانية منه، وقانون مملكة البحرين بشأن المعاملات الإلكترونية رقم (28) لسنة 2002 الذي سمّاها شهادة الاعتماد في المادة الأولى منه.

3 عمر حسن المومني، مرجع سابق، ص 61.

وسنذكرها في مكانها، لذلك سوف نستعين بقانون التوقيع الإلكتروني المصري لغرض معرفة البيانات التي يجب أن تحتويها شهادة التصديق الإلكتروني، حيث نصّت المادة (20) من اللائحة التنفيذية للقانون على هذه البيانات، وهذه الأخيرة منها ما هو متعلق بالموقع، ومنها ما يتعلق بجهة التصديق، ومنها ما يتعلق بشهادة التصديق نفسها[1].

أوّلاً: البيانات التي تتعلق بالموقع

فالبيانات التي تتعلق بالموقع مثل اسم الموقع الأصلي أو اسمه المستعار أو اسم شهرته، وذلك في حالة الاستخدام لأحدهم، وما يجب ملاحظته هنا أنّ المادة (46) من الترخيص رقم 103/ 2006 الصادر من هيئة صناعة تكنولوجيا المعلومات، والذي يتعلّق بخدمة التسجيل وإصدار الشهادات أجاز للموقع أن يطلب خطّيًّا من جهة التصديق حجب البيانات المتعلّقة به عن التداول كالاسم والعنوان وأيّ معلومات شخصية أخرى، والتي تدرجها جهة التصديق عادة بالدليل الذي تصدره، كذلك صفة الموقع حيث تقوم جهة التصديق بالتحقّق من صفة الموقع وإدراجها في الشهادة سواء كانت شخصية أم وظيفية، وذلك حسب الإجراءات التي نصّت عليها المادة (46) من الترخيص أعلاه، والمفتاح الشفري العام لحائز الشهادة والمناظر للمفتاح الشفري الخاص به، والهدف من ذكر هذا المفتاح هو أن يقوم الطرف الآخر المتعامل مع الموقع بمطابقة المفتاح العام المرسل إليه مع المفتاح العام المثبت في الشهادة، وبالتالي التأكّد من هوية الموقع[2].

---

1 مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثالث، مرجع سابق، ص 91.

2 سامح عبد الواحد التهامي، مرجع سابق، ص 478.

ثانيًا: البيانات التي تتعلّق بجهة التصديق

أمّا البيانات التي تتعلّق بجهة التصديق فتكون عبارة عن موضـــوع التـــرخيص الصادر للمرخص له، موضحًا فيه نطاقه ورقمه وتاريخ إصداره وفتـــرة ســـريانه، واسم الجهة المصدرة للشهادة وعنوانها ومقرّها الرئيسي وكيانها القـــانوني والدولـــة التابعة لها إن وجدت، والهدف كما يبدو من هذا البيان هو لتعريف الجهـــة وتحديـــد صفتها ومشروعيتها، وأن يكون التوقيع الإلكتروني لجهة إصدار الشهادة، والهـــدف من هذا هو لإثبات مصادقة جهة التصديق على صحة التوقيع الإلكتروني الموجـــود على المستند الإلكتروني ومحتوياته[1].

ثالثًا: البيانات التي تتعلق بشهادة التصديق

جاء في القانون الاتحادي رقم (1) لسنة 2006 بشـــأن المعـــاملات والتجـــارة الإلكترونية أنه يجب أن تحدّد شهادة المصادقة الإلكترونية هويـــة مـــزود خـــدمات التصديق، وأن الشخص المعينة هويته في شهادة المصادقة الإلكترونية لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في هذه الشـــهادة، وأن أداة التوقيـــع كانت سارية المفعول في أو قبل تاريخ إصدار شهادة المصادقة الإلكترونية، ومـــا إذا كانت هناك أيّة قيود على الغرض أو القيمة التي يجوز أن تستخدم مـــن أجلهـــا أداة التوقيع أو شهادة المصادقة الإلكترونية، وما إذا كانت هناك أيّة قيود على نطـــاق أو مدى المسؤولية التي قبلها مزود خدمات التصديق اتجاه أيّ شخص.

---

1 عباس العبودي، مرجع سابق، ص 22.

لقد أوجب قانون التوقيع الإلكتروني المصري تقديم ما يفيد صلاحية هذه الشهادة للاستخدام في التوقيع الإلكتروني، وهذا يعني أنّ شهادة التصديق تستعمل لأغراض التوقيع الإلكتروني دون الأغراض الأخرى.

وعن تاريخ بدء صلاحية الشهادة وتاريخ انتهائها حيث عادة ما تصدر الشهادات بفترة صلاحية محدودة وبمجرد انتهائها تصبح الشهادة غير صالحة للاستخدام ويتم رفضها تلقائيًّا من قبل برامجيات المرسل إليه، والهدف من وراء إدراج هكذا بيان هو التأكد من أن التوقيع الإلكتروني قد تم إنشاؤه أثناء فترة الصلاحية أم لا[1].

وقد أجاز الترخيص رقم (103/ 2006) لجهة التصديق تقديم خدمة البصمة الإلكترونية التي يتم من خلالها تسجيل وقت وتاريخ إنشاء وتثبيت التوقيع الإلكتروني بشكل دقيق، كذلك تفيد بإمكانية الفحص والتحقّق من بيانات إنشاء التوقيع الإلكتروني خلال وقت وتاريخ محدّدين، ويتم تقديم هذه الخدمة مقابل ثمن تحدّده الهيئة حسب قائمة أسعار معيّنة.

إنّ كلّ شهادة تصدر من جهة التصديق تحمل رقمًا تسلسليًّا معيّنًا، والغرض من وضع هذا البيان هو تمييز السندات الإلكترونية الصادرة من أصحابها عن غيرهم من الموقّعين، وبذلك تصبح قراءة الرسائل الإلكترونية والسندات الإلكترونية أمرًا محصورًا على أطراف المعاملة دون غيرهم، وهذا الأمر يضفي الثقة على السند أو المحرر الإلكتروني، وكذلك التصرف القانوني الذي تم من خلاله، كذلك يفيد هذا البيان بأن منشئ السند هو الشخص الوحيد الذي يستطيع كتابته والتعديل فيه والتوقيع

---

1 المحامية عبير ميخائيل الصفدي الطوال، التوقيع الإلكتروني، دار وائل للنشر والتوزيع، عمان – الأردن، ط 1، 2010م، ص 104.

عليه، كما يضمن للموقع أنّ المرسل إليه هو الشخص الوحيد الذي يستطيع قراءة السند دون قدرته على التعديل عليه[1].

كذلك عنوان الموقع (web site) المخصّص لقائمة الشهادات الموقوفة أو الملغاة حيث نصّت المادة (45/ 12/ ز) من الترخيص رقم (103/ 2006) على التزام جهة التصديق بوضع نظام خاص لإيقاف الشهادة أو إلغائها، وعندما يتم إيقاف أو إلغاء أيّة شهادة يتم إضافتها إلى قائمة الشهادات الملغية أو الموقوفة، والتي يتم نشرها على الموقع الخاص بذلك، وبخلاف ذلك تتحمّل جهة التصديق كافة التبعات الناتجة عن قيام أحد المستخدمين بالتوقيع معتمدًا على شهادة ملغاة أو موقوفة ولم يتم نشرها عبر الموقع الإلكتروني المخصّص لهذا الغرض. وبالإضافة إلى ما تقدّم من بيانات جاء باللائحة التنفيذية بيانات اختيارية أخرى يجوز إدراجها عند الحاجة مثل ما يفيد اختصاص الموقع والغرض الذي تستخدم فيه الشهادة، ووضع حدّ لقيمة التعاملات المسموح بها بالشهادة، ومجالات استخدام الشهادة.

وتستخدم هذه البيانات حسب الغرض من إصدار الشهادة، حيث إنّ شهادات التوثيق تختلف من حيث وظيفتها، فمنها ما يستخدم في تعامل معيّن ذو قيمة مالية منخفضة، يتطلب إصدارها أن يقدم المشترك عنوانًا إلكترونيًّا صالحًا للاستخدام، كما إنّ هناك شهادات تستخدم من قبل أشخاص مخوّلين بالتوقيع عن شركات أو هيئات معينة[2].

---

1 عباس العبودي، مرجع سابق، ص 221.

2 عمر حسن المومني، مرجع سابق، ص 65.

لذلك نجد أنّ توافر هذه البيانات أو عدم توافرها يعتمد على الغرض الذي تستخدم من أجله الشهادة ومجال استخدامها ونوعها.

ولضمان صحة التوقيع الإلكتروني ونسبته لصاحبه، هناك ضوابط وشروط اعتمدت عليها جهات التوثيق، منها[1] أن يكون التوقيع خاصًّا ومرتبطًا بشخص الموقع، وتم إنشاؤه بوسائل خاصة بالشخص، وتحت سيطرته، وأن يرتبط بالسجل الذي يتعلّق به بصورة لا تسمح بإجراء تعديل على قيد بعد توقيعه دون أحداث تغير في التوقيع، ومن الممكن أن يثبت هوية ذلك الشخص.

يتّضح من خلال ما سبق أن جهات التصديق الإلكتروني تضمن مصداقية الشهادة الإلكترونية وصحة السندات والتواقيع الإلكترونية وسلامتها، ويؤدّي ذلك إلى توطيد الثقة بين المتعاملين لإبرام صفقات إلكترونية من خلال الشبكة المفتوحة وإثباتها بسهولة.

1 آزاد دزه يي، مرجع سابق، ص 123.

الفصل الثاني

شروط حجية التوقيع الإلكتروني وآثاره في الإثبات

تمهيد وتقسيم:

عندما يبرم الأطراف عقودًا بطريقة إلكترونية فإنهم يوقّعون عليها توقيعًا إلكترونيًّا، كما أنّ أيّة مراسلات تتم بينهم لا بد أن تكون موقّعة إلكترونيًّا، وعليه لا بد أن نتعرّض لحجية التوقيع الإلكتروني للأطراف في مواجهة بعضهم البعض، وإذا كان الهدف من موجة التشريعات الحديثة هو تسهيل استعمال الوسائل الإلكترونية في المعاملات التجارية، فإنّ أبرز صور هذا المدّ التشريعي جاءت بالأساس لتحسين أنظمة الإثبات في القوانين المدنية المعاصرة، كما أنّ أسمى أهداف مواءمة أنظمة الإثبات مع متطلّبات المعاملات الإلكترونية هو الاعتراف القانوني بالوثيقة الإلكترونية وإعطائها نفس الحجية القانونية التي تتمتع بها الوثيقة الكتابية العادية.

والاعتراف بالوسائل الإلكترونية في التعاقد والإثبات ومنحها الحجية والمقبولية المقررة لوسائل التعاقد والإثبات القائمة في البيئة غير الإلكترونية، اتخذ مستويات متطورة، وفيما يأتي سأتطرق إلى الحديث عن شروط حجية التوقيع الإلكتروني وآثاره من خلال المباحث الآتية:

المبحث الأول: شروط حجية التوقيع الإلكتروني

المبحث الثاني: الآثار المترتبة على توافر شروط حجية التوقيع الإلكتروني

المبحث الثالث: وظيفة التوقيع الإلكتروني ودوره في الإثبات

المبحث الأول
شروط حجية التوقيع الإلكتروني

تمهيد وتقسيم:

رغم رغبة التشريعات المختلفة في إضفاء الحجية على التوقيعات الإلكترونية والرسائل الإلكترونية، فإنها تأخذ ذلك بحذرها وتختلف في منهجها من حيث الشروط الواجب توافرها في إضفائها الحجية عليها وبيان مجال استخدامها، وكذلك في التنظيمات الخاصة بالتوثيق والتفاصيل الخاصة بها، بحيث يتعيّن إجراء المقارنة فيما بينها، والعمل على توحيد الدعامات الرئيسية المهيّأة للأخذ بهذا التنظيم بثقة واطمئنان، وذلك مع الأخذ بمبدأ الحيدة بين التقنيات التكنولوجية المتاحة لتحقيق شروط حجية التوقيع الإلكتروني.

وحتى يتمتّع التوقيع الإلكتروني بحجية في الإثبات لا بد أن يستوفي الشروط التي تمنحه الحجية القانونية في الإثبات، والتي يؤدّي عدم توافرها إلى عدم تحقّق وصف التوقيع الإلكتروني، وذلك من خلال تحديد هوية الموقِّع والتأكّد من صحة التوقيع وصلاحيته للاحتجاج به قانونًا، كونه يعبّر عن إرادة الأطراف في التصرّف، وسوف أتناول في هذا المبحث شروط حجية التوقيع الإلكتروني من خلال المطلبين الآتيين:

المطلب الأول: شروط تمتّع التوقيع الإلكتروني بالحجية

المطلب الثاني: توثيق التوقيع الإلكتروني ونطاقه

المطلب الأول: شروط تمتّع التوقيع الإلكتروني بالحجية

يمرّ التوقيع الإلكتروني بمرحلتين: الأولى تتعلّق بإنشاء التوقيع، وتوفير التأمين اللازم لذلك، والثانية مرحلة التحقّق من صدوره من الموقع، وذلك عند تلقي الرسالة الإلكترونية غير أنه حتى تتحقّق الحجية القانونية للتوقيع الإلكتروني، ويكون له ذات الحجية للتوقيع التقليدي، يتعيّن توافر عدة شروط، فضلاً عن وجوب اشتراك طرف ثالث غير الراسل والمرسل إليه، يضطلع بمهمة إصدار شهادات التوثيق التي تنفذ صدور التوقيع من الموقع، ومن ثم التعرف على هويته ونسبة الرسالة والتوقيع له.

الفرع الأول: شروط التوقيع الإلكتروني المعتمد

أولاً: أن يكون التوقيع متميزًا ومرتبطًا بشخص الموقع:

التوقيع الخطي عبارة عن إشارة خطية متميزة خاصة بالشخص الذي صدرت عنه، والذي اعتاد أن يستعملها للإعلان عن اسمه[1].

ففي التوقيع الإلكتروني يجب أن تكون أداوت إنشاء التوقيع، من رموز وأرقام وغيرها متميزة بشكل فريد ومرتبطة بالشخص الموقع وحده دون غيره، لضمان عدم قيام أيّ شخص آخر بإنشاء التوقيع نفسه، لارتباط التوقيع بصاحبه ارتباطًا وثيقًا معنويًّا وماديًّا بالارتباط بين البيانات المستخدمة لإنشاء التوقيع، والموقع هو العنصر

---

1 إلياس أبو عبيد، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، الجزء الأول، منشورات الحلبي الحقوقية، 2005م، ص181.

الرئيسي[1]. وهو ما نجده في أعظم صور التوقيع الإلكتروني، باعتبار أن التقنية المستخدمة فيه تعتمد على البيانات الشخصية للموقع، فمثلاً التوقيع البيومتري للموقع، وكذلك الشأن في التوقيع بالرقم السري فكل رقم سري يقابله شخص وحيد، وفي التوقيع الرقمي المفتاح العام والخاص المميزين لشخص الموقع.

ثانيًا: أن يكون التوقيع محدّدًا لشخص الموقع.

يعدّ هذا الشرط أمرًا بديهيًّا لا بد منه باعتباره من وظائف التوقيع بالمفهوم العام، فالتوقيع الإلكتروني يجب أن يكون محدّدًا لهوية شخص الموقع على الرسائل الإلكترونية، ويتحقّق بذلك من خلال الرجوع إلى الجهات التي تقوم بإصدار شهادات التوثيق المعتمدة ممّن يريد إنشاء توقيع إلكتروني، للتأكّد من هوية الشخص الذي يستخدم التوقيع[2].

وهو ما نصّ عليه قانون الأونسيترال النموذجي[3] "يعتبر التوقيع الإلكتروني قابلاً للتعويل عليه، إذا كانت بيانات إنشاء التوقيع مرتبطة في السياق الذي يستخدم فيه الموقع دون أي شخص آخر".

ثالثًا: سيطرة الموقع على منظومة التوقيع.

ويقصد به من الناحية الفنية سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني المستخدم في عملية تثبيت التوقيع الإلكتروني[4]، حتى يضمن أن يكون

---

1 علاء محمد نصيرات، مرجع سابق، ص 133.

2 علاء محمد نصيرات، مرجع سابق، ص 134.

3 المادة (3/6) بند (أ) من قانون الأونسيترال النموذجي لسنة 2001.

4 محمد أمين الرومي، مرجع سابق، ص 61.

صاحب التوقيع منفردًا بذلك التوقيع سواء عند التوقيع ذاته أم استعماله بأيّ شكل من الأشكال[1].

وهو ما نصّ عليه قانون الأونسيترال النموذجي[2] "على أن تكون بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون غيره".

وهذا الشرط يستلزم وجوب خضوع أدوات إنشاء التوقيع الموثق بأيّ صورة من صوره، لسيطرة صاحب التوقيع ولزوم رعايته لها بعدم نشرها والإفصاح عنها لصالح الغير حفاظًا على سلامة المستندات الموقعة إلكترونيًّا، ومثال ذلك أن من يستعمل البطاقات البلاستيكية (الممغنطة) عليه الاحتفاظ بسرية رقمه المعطى له لقبول دخوله والقيام بالعمليات المصرفية، وإلا أمكن استعمال البطاقة من شخص أجنبي، وكذلك الأمر في التوقيعات الرقمية، إذ يجب تأمين وحماية المفتاح الخصوصي وإبقائه سرّيًّا.

رابعًا: ارتباط التوقيع بالسند الذي يتعلّق به مع إمكانية كشف أيّ تبديل أو تعديل في بيانات التوقيع الإلكتروني

يتناول هذا الشرط مسألة سلامة التوقيع الإلكتروني، وسلامة المعلومات التي يوقع عليها صاحب التوقيع إلكترونيًّا، حيث إذا تم التوقيع على المستند الإلكتروني فإنّ سلامته وسلامة التوقيع مرتبطين ارتباطًا وثيقًا ببعضهما[3].

---

1 عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص 444.

2 المادة (3/6) البند "ب" من قانون الأونسيترال النموذجي لسنة 2001.

3 علاء محمد نصيرات، مرجع سابق، ص 136.

وهو ما نصّ عليه قانون الأونسيترال النموذجي[1] "إذا كان أيّ تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلاً للاكتشاف".

الفقرة "د" كان الغرض من اشتراط التوقيع قانونيًّا هو تأكيد سلامة المعلومات التي يتعلّق بها التوقيع، وكان أيّ تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلاً للاكتشاف".

وتضمين التوقيع الإلكتروني في السند الإلكتروني له طابعًا خاصًّا، يتلاءم مع البيئة الإلكترونية ففي التوقيع الإلكتروني لا يوجد اتصال محسوس بين البيانات المكونة للكتابة وبيانات التوقيع فيما بينهما، وبين الدعامة التي يظهران فيها، فكلّ منها كيان معلوماتي مستقل، لكن مع ذلك لا بد من ارتباطهما ارتباطًا منطقيًّا يمكن من تحديد هوية الموقع والتعبير عن إرادته في قبوله بمضمون السند، مع إمكانية الكشف عن أيّ تغيير في التوقيع في أيّ لحظة، كما أن هذا الارتباط لا يسمح بإجراء تعديل في السند الموقع دون إحداث تغيير على التوقيع[2].

خامسًا: الاستيثاق من مضمون المحرر الإلكتروني.

يجب توافر موثوقية الوسيلة المستخدمة في التوقيع من أجل الاعتراف القانوني بالتوقيع الإلكتروني، ومنحه الحجية المقررة للتوقيع الخطي في مجال الإثبات، حيث أشار القانون المدني الفرنسي[3] "افتراض موثوقية هذه الوسيلة إلى أن يثبت عكس ذلك، بمجرد إنشاء التوقيع الإلكتروني الذي تتحدّد بموجبه هوية الموقع، ويضمن

---

1 المادة (3/6) بند "د" الفقرة "ج" من قانون الأونسيترال النموذجي لسنة 2001.

2 علاء محمد نصيرات، مرجع سابق، ص 137.

3 المادة (1316/ 4) مدني فرنسي.

سلامة المحرر، وذلك بالشروط التي يحدّدها مرسوم يصـــدر عـــن مجلـــس الدولـــة الفرنسي، ويلاحظ على هذا النص أنه لم يشر إلى المقصود بالموثوقية، وإنما وضـــع قرينة بافتراض موثوقية الطريقة المستخدمة في التوقيع بقدر استيفائها للشروط التـــي يحددها المرسوم المنوه عنه، ولا شك أن هذا النص يعكس تخوف المشرع من مـــنح ثقة مطلقة لنظام تصديق خاص بمقدمي خدمات التصديق الإلكتروني.

وفي الاتجاه ذاته أكّد المرسوم الصادر عن مجلـــس الدولـــة الفرنســـي بتـــاريخ 2001/3/30م بشأن تطبيق نص المادة (4/1316) من القـــانون الفرنســـي علـــى افتراض موثوقية الوسيلة المستخدمة في التوقيع الإلكتروني إلى أن يثبت عكس ذلك، غير أنّ هذا المرسوم لم يكتف بهذا الحد، وإنما ذهب أبعد من ذلك حين نـــصّ علـــى شروط موثوقية تلك الوسيلة التي تتلخّص في أن تنشأ هذه الوسيلة توقيعًا إلكترونيًّـــا مؤمنًا، وضرورة أن يكون خاصًّا بالموقع، وأن ينشأ بواسطة وسائل يمكن أن يحتفظ بها الموقع تحت سيطرته، وأن يكفل رابطه مع المحرر المتصل بـــه بحيـــث يمكـــن كشف أيّ تعديل لاحق على المحرر[1]، ثم أوجب المرسوم السالف الـــذكر أن ينشـــأ التوقيع الإلكتروني المؤمن بفضل منظومة إنشاء توقيع إلكتروني مأمونة، ومنظومـــة للتحقّق من صحة التوقيع الإلكتروني تعتمد على استخدام شهادة تصديق مؤهلة.

وهكذا يتّضح من أحكام النصوص المذكورة أن قرينة الموثوقيـــة لا تـــرتبط إلا بتوقيع إلكتروني مؤمن؛ أي: التوقيع الذي يستوفي المقتضيات القانونية الواردة فـــي المادة (4/1316) من القانون المدني ونصوص المرسوم المشار إليه المنفذة لهـــا[2]،

---

1 المادة الأولى الفقرة الثانية من مرسوم مجلس الدولة رقم 272/ 2001م.

2 مرسوم مجلس الدولة الفرنسي رقم 272/ 2001م.

أمّا إذا ثبت أن التوقيع الإلكتروني المؤمن معيب فلا يعني ذلك أنــه عــديم الفائــدة القانونية، غير أنّ الفقه انقسم حيال هذه المسالة، فالبعض ذهب إلى أنه يمكن أن يأخذ قيمة مبدأ الثبوت بالكتابة[1]، والحكم ذاته ينطبق على التوقيع البسيط، فبــالرغم مــن عدم تمتّعه بقرينة التكافؤ مع التوقيع الخطي، فإنه يأخذ حكم مبدأ ثبوت بالكتابة، لأنّ الأولى إعماله ولا يمكن أن يكون عديم القيمة القانونية، ويمكن حينئذ أن يستكمل بأيّ وسيلة إثبات كالبينة والقرائن، في حين يرى البعض الآخر أن يترك تقــدير حجيــة التوقيع الإلكتروني المعيب وما يتوافر فيه مــن عناصــر أمــان لســلطة القاضــي التقديرية[2]، في ضوء ظروف كل حالة على حدة، قياسًا على ما قضت بــه المــادة (228/ 1) الجديدة من قانون المرافعات المدنية الفرنسي، وبخاصــة أن المرســوم الصادر بتاريخ 2001/3/30م مستمد أحكامه من التوجيه الأوروبي الصادر في 13 ديسمبر 1999م بشأن الإطار العام للتوقيعات الإلكترونية، وأنّ ذلك التوجيــه يلــزم الدول الأعضاء- وفرنسا من بينهم- بعدم إنكار القيمة القانونيــة لوســيلة التوقيــع الإلكتروني وحجيتها في الإثبات لمجرد أنها وردت في الشــكل الإلكترونــي، أو لا تعتمد على شهادة تصديق مؤهلة، أو صادرة بواسطة مقدم خدمات غير معتمــد، أو لأنه لم ينشأ بواسطة منظومة إنشاء توقيع إلكتروني "المادة الثانية" من التوجيه.

1 تامر محمد سليمان الدمياطى، إثبات التعاقد الإلكترونى عبر الإنترنت: دراسة مقارنة، منشأة المعارف، 2009م، ص 418. يمكننا تعريف مبدأ الثبوت بالكتابة كما عرفه قانون الإثبات في المعاملات المدنية والتجارية في المادة 37 بأنه يجوز الإثبات بشهادة الشهود فيما كان يجب إثباته بالكتابة إذا وجد مبدأ ثبوت بالكتابة، ويعتبر مبدأ ثبوت بالكتابة كلّ كتابة تصدر من الخصم ويكون من شأنها أن تجعل وجود التصرف المدعي به قريب الاحتمال.

2 تامر محمد سليمان الدمياطى، المرجع السابق.

باختصار متى كان التوقيع الإلكتروني المؤمن مستوفيًا للشروط الواردة في الفقرتين الأولى والثانية من المادة (1316 /4) مدني، وأحكام المرسوم الصادر بتاريخ 2001/3/30م بشأن وضع هذه المادة الأخيرة موضع التطبيق، فالتوقيع الإلكتروني في هذه الحالة يكون موجبًا بالأمان ومحلاً للثقة، هذا وقد استلزم هذا المرسوم الأخير إنشاء جهة تختصّ بتقديم خدمات التصديق على التوقيع الإلكتروني، كما تناول في الوقت ذاته جملة من الأحكام تحدّد نظام عملها، والتزاماتها ومسؤولياتها.

الفرع الثاني: شروط سلامة التوقيع الإلكتروني

يجب أن تتوافر في التوقيع الإلكتروني عدة شروط عامّة تضمن سلامته وأمانه وبعده عن يد العبث والتزوير، وذلك حتى يمكن الاعتداد به قانونًا فيجب أن يكون للتوقيع الإلكتروني طابعًا يتفرّد به، بحيث يسمح بتحديد شخصية الموقع وتمييزها عن غيرها، وذلك باستخدام تقنية آمنة تضمن ذلك، وأن تضمن التقنية المستخدمة صلة الموقع بالتصرف القانوني المرتبط به بل لا بد أن يرتبط التوقيع الإلكتروني بالموقع وحده دون غيره، ويتم ذلك عن طريق سيطرة الموقع على الوسيط الإلكتروني، وضرورة الحفاظ على صحة المحرر الإلكتروني، وذلك بتوفير وسيلة لكشف أيّ تعديل أو تبديل في بيانات المحرّر أو في التوقيع الإلكتروني الوارد عليه[1].

إنّ الاستدلال على التوقيع يكون من خلال عنصرين: شكلي وموضوعي، يتمثّل العنصر الشكلي في أن التوقيع علامة مميزة وخاصة بصاحبها أيًّا كانت هذه العلامة،

---

1 أسامة روبي عبد العزيز الروبي، مرجع سابق، ص 20.

أمّا العنصر الموضوعي أو الوظيفة القانونية، وهو الأهم، فيتلخّص في أن للتوقيع وظيفه ذات بعدين، هما: تحديد هوية صاحب السند، وموافقة الموقع عليه واتجاه إرادته للالتزام بموجبات مضمونه أو إذعانه شخصيًّا لمحتوى هذا السند[1].

وفي مجال التعاملات الإلكترونية الحديثة وإتمام المعاملات المالية وإبرام العقود عبر الإنترنت، لم يعد التوقيع التقليدي يتلاءم مع مستجدات التطور الحاصل في كثير من مجالات التعامل، إذ إنّ معظم المعاملات تتم بواسطة وسائل الاتصال الحديثة معتمدة في ذلك على الكتابة الإلكترونية والمحررات الإلكترونية، لذا كان من الضروري توثيق هذه المحررات من أطراف التعاقد بواسطة توقيع يتناسب مع طبيعة الوسط، ويرى البعض أننا إذا تمسّكنا بالتوقيع التقليدي أو الكتابي، فإنّ هذا يعني توقّف معظم أو كلّ الأنشطة التجارية التي تجري عبر الإنترنت، الأمر الذي يعدّ ضربة في عصب الاقتصاد العالمي، ويهدّد بانهياره. لذلك يجب قبول التوقيع الإلكتروني وإعطاءه الحجية القانونية في الإثبات مثله مثل التوقيع الكتابي، فالتوقيع بالمعنى المفهوم وفقًا لنصوص قانون الإثبات الحالي لا يستوعب أساليب التعامل الحديثة، لهذا كان من الضروري الأخذ بتوقيع يتناسب مع طبيعة الوسط، ومن ثمّ وجد التوقيع الإلكتروني[2].

---

1 وسيم شفيق الحجار، الإثبات الإلكتروني، بيروت، 2002م، ص 139.

2 محمد المرسي زهرة، مدى حجية التوقيع الإلكتروني في الإثبات، مؤتمر الكمبيوتر والقانون، كلية الحقوق، جامعة عين شمس، فبراير 1994م، ص89.

المطلب الثاني: ضوابط توثيق التوقيع الإلكتروني ونطاقه

يفرض لاستخدام التوقيع الإلكتروني بطريقة آمنة وموثوقة، لا بد من وجود جهة موثوق بها، لربط شخص أو كيان بالتوقيع، ويتمّ ذلك عن طريق جهات التوثيق التي تصدر شهادات التوثيق، لإثبات نسبة التوقيع الإلكتروني إلى شخص معيّن استنادًا إلى إجراءات التوثيق المعتمدة، أو المتّفق عليها بين الأطراف[1].

والغرض من إجراءات التوثيق هو التحقّق من أنّ التوقيع الإلكتروني لم يطرأ عليه تعديل أو تغيير، وهو ما يؤدّي إلى إعطاء التوقيع الإلكتروني الحجية القانونية في مواجهة أطرافه والغير[2]، وتكون جهات التوثيق مسؤولة عن صحة المعلومات الموثقة بالشهادات التي تصدرها، وعن صحة الربط بين الموقع والتوقيع الإلكتروني.

الفرع الأول: ضوابط توثيق التوقيع الإلكتروني

تجدر الإشارة إلى أنّ التوقيع الإلكتروني غير المصادق على صحته من جهات التصديق، لا تنعدم قوته الثبوتية لإعطائه الحجية وتمتعه بالآثار القانونية للتوقيع الصحيح، وعليه يجب أن تنتظم هيئات المصادقة الجهة المكلّفة بتحديد بتوثيق التوقيع الإلكتروني، إذ لا يتصور ثقة الأفراد في وسيلة لا توفر أدنى ضمان، الأمر الذي يحدّ من تفعيل هذه النصوص بشكلها الحالي.

---

1 خالد ممدوح إبراهيم، مرجع سابق، ص 196 وص 197.

2 علاء محمد نصيرات، مرجع سابق، ص 126.

ويلاحظ أنّ التشريعات التي نصّت على الأخذ بالتوقيع الإلكتروني، وفي سبيل إضفاء صفة أو عنصر الأمان عليه اتخذت وسائل تضمن ثقة المتعاملين بها[1]، كما جعلت لها قوة في الإثبات مساوية للتوقيع التقليدي، غير أنه لا محل لهذه القوة إلا إذا توافرت ضوابط تكفل ضمان صحة التوقيع وسلامته، ولتحقيق هذا الهدف أصدرت قوانين ولوائح إدارية تتضمّن الضوابط والإجراءات الواجب اتخاذها بشأن استخدام التوقيع الإلكتروني وتوثيقه، وتتمثّل هذه الضوابط فيما يأتي[2]:

1. الضوابط الفنية العامة:

هناك عدة ضوابط فنية عامة يجب أن تتوافر في التوقيع الإلكتروني، فيجب أن يكون التوقيع خاصًّا بالشخص وحده ولا يشاركه فيه غيره، كما يجب ألا يكون قد سبق استخدام هذا التوقيع من قبل حتى لو من صاحبه، وعلة ذلك هي كفالة أكبر قدر من السرية على هذا التوقيع، ويجب على الشخص صاحب التوقيع أن يقرّ كتابة بأنّ توقيعه الإلكتروني ملزم قانونًا ويتساوى مع توقيعه بخط اليد من حيث الأثر القانوني، غير أنّ هذا الإقرار غير لازم في كلّ مرة يضع فيها الشخص توقيعه الإلكتروني. ويجوز للهيئة المسؤولة عن التوقيع الإلكتروني أن تطلب من صاحب التوقيع أن يقدم شهادة بصحة توقيعه بمناسبة تصرف معيّن، وفي هذه الحالة فإنه

---

1 فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، المنظمة العربية للتنمية الادارية، 2005م، ص243.

2 أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، منشور على الموقع الإلكتروني http://www.startimes.com/?t=17717139 تاريخ الاطلاع 14-02-2017م.

يجب عليه تقديمها، ويخضع التزوير في هذه الشهادة للقواعد العامة في جريمة التزوير.

2. الضوابط الفنية الخاصة:

إلى جوار الضوابط العامة سالفة الذكر، فإنه توجد ضوابط فنية خاصة للتوقيع الإلكتروني، وهي تختلف من نظام تشريعي إلى آخر بحسب ما توفّره من أمن وسلامة المعاملات من ناحية، ومرونة وعدم عرقلة هذه المعاملات من جهة أخرى، وتتّصل هذه الضوابط بتشفير المستند، سواء أكان توقيعًا أم سجلاً إلكترونيًّا، ويلاحظ أنه لا يكفي لضمان سلامة إتمام المعاملة الإلكترونية أن يتم تشفير الرسالة المنسوبة لشخص معيّن، وإنما يجب التأكّد من نسبة هذه الرسالة لهذا الشخص، وأنّ مضمونها لم يتعرّض لتبديل أو تشويه.

الفرع الثاني: نطاق حجية التوقيع الإلكتروني

قامت معظم الدول التي أصدرت تشريعات خاصة بالتوقيع الإلكتروني إدراج شروط خاصة أخرجت من نطاقها بعض المعاملات، ولم تقبل فيها التوقيع الإلكتروني حتى لو كانت مستوفية لكافة الشروط، واقتصرت على البعض الآخر، وذلك على التفصيل الآتي:

1. موقف المشرع الإماراتي والتشريعات المقارنة من المعاملات التي يقبل فيها التوقيع الإلكتروني:

نصّ قانون المعاملات والتجارة الإلكترونية لإمارة دبي على[1] أنه "يسري قانون المعاملات والتجارة الإلكترونية على السجلات والتواقيع الإلكترونية ذات العلاقة بالمعاملات والتجارة الإلكترونية".

في حين أنّ القانون المصري الخاص بالتوقيع الإلكتروني، قد نصّ في المواد (14، 15) على أنّ التوقيع الإلكتروني له الحجية في الإثبات المنصوص عليها في قانون الإثبات إذا ما تمّ استخدامه في المعاملات التجارية والمدنية والإدارية فقط، ولم ينصّ على حجيته في الإثبات إذا استخدم في المعاملات الأخرى التي تخرج عن نطاق المعاملات المدنية والتجارية والإدارية[2].

لذا نرى أن المشرع المصري حدّد نطاق استخدام التوقيع الإلكتروني في أحكام قانون الإثبات في المواد المدنية والتجارية على التوقيع الإلكتروني، وذلك في المعملات المدنية والتجارية، وهو بذلك يكون قد توسّع في هذا النطاق من حيث المعاملات التي تنصرف إليها هذه الحجية إلا أنه حدّدها من جانب آخر من حيث النطاق في حدود الحجية المقررة للتوقيعات في المواد المدنية والتجارية، وعلّق سريان هذه الحجية على أن يراعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحدّدها اللائحة التنفيذية لهذا القانون، وذلك يوضّح وجود خلاف بين التشريعات حول نطاق استخدام التوقيع الإلكتروني، فقد أقرّت بعض الدول استخدامه في المعاملات المدنية والتجارية فقط، ومنها من أقرّ

---

1 المادة 5 من القانون رقم 2 لسنة 2002 بشأن المعاملات والتجارة الإلكترونية الإماراتي.

2 منيرمحمد الجنبيهي، ممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، الإسكندرية، 2005م، ص 96.

استخدامه في المعاملات مع الجهات الحكومية، ومنها من جمع بين الاثنين، فالتشريع الأمريكي والإماراتي عمدا إلى فتح المجال أمام الدوائر الحكومية والمؤسسات الرسمية، لاستخدام الوسائل الإلكترونية في إنجاز المعاملات المختلفة التي تدخل ضمن نشاطاتها، وذلك بصورة كلية أو جزئية، وهو ما يعرف بمصطلح الحكومة الإلكترونية، حيث يمكن إنجاز معظم الخدمات التي تقدّمها عن طريق الوسائل الإلكترونية، وهو ما يجعلها تستخدم التوقيع الإلكتروني في أداء الخدمة الإلكترونية، حتى تكون هذه المعاملات كاملة من الناحية القانونية.

إنّ قانون الأونيسترال قد أقرّ أن قواعده تطبق عندما يستخدم التوقيع الإلكتروني في سياق الأنشطة التجارية؛ أي: جعله حجة في الإثبات التجاري فقط، أخذا بذلك بالمفهوم الواسع للمصطلح "تجاري"[1].

فضلاً على اعتراف معظم التشريعات بسريان التوقيع الإلكتروني في المعاملات التي يتّفق فيها الأطراف على إجرائها بالوسائل الإلكترونية، وهو ما يشمل جميع المعاملات المدنية والتجارية في غياب ما يستثنيها بنص قانوني، وذلك متى استوفى التوقيع الإلكتروني لجميع الشروط والأوضاع التي اشترطها القانون[2].

1 قانون الأونسيترال النموذجي بشأن التوقيع الإلكتروني.

2 علاء محمد نصيرات، مرجع سابق، ص 162، 164.

2. موقف المشرع الإماراتي والتشريعات المقارنة من المعاملات التي لا يقبل فيها التوقيع الإلكتروني:

نصّ قانون المعاملات والتجارة الإلكترونية لإمارة دبي على[1] أنه "يسري قانون المعاملات والتجارة الإلكترونية على السجلات والتواقيع الإلكترونية ذات العلاقة بالمعاملات والتجارة الإلكترونية، ويستثنى من أحكام هذا القانون[2] المعاملات والأمور المتعلقة بالأحوال الشخصية كالزواج والطلاق والوصايا، وسندات ملكية الأموال غير المنقولة، والسندات القابلة للتداول، والمعاملات التي تتعلق ببيع وشراء الأموال غير المنقولة والتصرف فيها وتأجيرها لمدد تزيد على عشر سنوات، وتسجيل أيّة حقوق أخرى متعلقة بها، وأيّ مستند يتطلب القانون تصديقه أمام الكاتب العدل.

أمّا القانون السعودي فقد استثنى بعض المعاملات بنصه عليها[3] "يسري هذا النظام على التعاملات والتوقيعات الإلكترونية ويستثنى من أحكامه التعاملات المتعلقة بالأحوال الشخصية، وإصدار الصكوك المتعلقة بالتصرفات الواردة على العقار،

---

1 المادة (5) من القانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية لإمارة دبي.

2 مجدي أحمد عزام، المحامي بالنقض والإدارية العليا محاضر بمعهد المحاماة بالإسكندرية دراسات عليا في القانون صاحب إصدارات قانونية مسجلة بدار الكتب، منتدى المحامين العرب المنتدى العام بحث عن الحجية القانونية للتوقيع الإلكتروني والمعاملات الإلكترونية في القوانين العربية "دراسة مقارنة" منشور على الموقع الإلكتروني، تاريخ الاطلاع عليه: 20-2-2017م.
http://www.mohamoon.com/MONTADA/Default.aspx?Action=Display&ID=117932&Type=3

3 المادة (3) من نظام التعاملات الإلكترونية السعودي.

وذلك ما لم يصدر من الجهة المسؤولة عن هذه التعـــاملات مـــا يســـمح بإجرائهـــا إلكترونيًّا، وفق ضوابط تضعها تلك الجهة بالاتفاق مع الوزارة.

فالملاحظ أنّ المنظم السعودي في نظام التعاملات الإلكترونية أجاز للدوائر الحكومية والرسمية إجراء معاملاتها جميعًا أو جزءًا منها بوسائل إلكترونية، فإذا ما قامت إحدى الدوائر بذلك فإنّ نظام التعاملات الإلكترونية سوف ينطبق على هذه المعاملات جميعًا، وسواء كانت هذه المعاملات ذات طابع تجاري أم مدني، وعليه فإنّ المنظم السعودي لم يحدّد سريان نظام التعاملات الإلكترونية فقط على الأنشطة التجارية، كما فعل قانون اليونسيترال بل جاء النص عامًّا دون تخصيص، وهذا يعد توسعًا من المنظم في سياق التوجه نحو الحكومة الإلكترونية التي ظهرت حديثا، وبدأ تطبيقها في كثير من دول العالم، وحيث إنّ المعاملات التي تتم عن طريق الحكومة الإلكترونية تحتاج إلى استخدام التوقيع الإلكتروني المدعم بشهادة توثيق من الجهات المختصّة للتحقّق من شخص المتعامل معها، والجهة الحكومية التي تؤدّي الخدمة بحاجة أيضًا إلى استخدام التوقيع الإلكتروني حتى تكون إجراءاتها قانونية[1].

كذلك فإنّ الملاحظ من نظام التعاملات الإلكترونية أنّ تنظيم السندات الرسمية كأصل عام جائز إلا أن المنظم السعودي قد قرن هذه الإمكانية بمدى اعتماد الدوائر الحكومية على إجراء معاملاتهم إلكترونيًّا وتنظيمها، فأجاز المنظم ذلك وفق ضوابط معينة بأن تقوم إحدى الدوائر الحكومية بتنظيم سنداتها إلكترونيًّا، وبالتالي، إذا أعلنت

1 علاء محمد نصيرات، مرجع سابق، ص 162، وما بعدها.

إحدى الدوائر الرسمية رغبتها بإتمام معاملاتها الرسمية إلكترونيًّا فإنّ ذلك جائز قانونًا كأصل عام[1].

وكلّ ذلك شرط ألاّ تكون هذه المعاملة من المعاملات التي استثناها المنظم من التوقيع، ومن الملاحظ أن المنظم السعودي ترك للأطراف حرية الاختيار في إبرام عقودهم بوسائل إلكترونية، فإذا ما اتفق الأطراف على اختيار الوسائل الإلكترونية كوسيلة لإثبات اتفاقهم فإنّ هذا الاتفاق يكون ملزمًا لهم، وبالتالي لا يجوز لهما إثبات هذا الاتفاق بغير هذه الوسيلة إعمالاً لقاعدة العقد شريعة المتعاقدين.

من خلال نصّ المادة (3) من نظام التعاملات الإلكترونية السعودي نرى هناك حصرًا للمعاملات المستثناة من التعامل بوسائل إلكترونية من ضمنها التعاملات المتعلّقة بالأحوال الشخصية. والصكوك المانعة من التصرفات الواردة على العقار، وأرى أن النظام راعى دخول الحاسوب الإلكتروني إلى معظم الدوائر الحكومية كالمحاكم، ووزارة الداخلية وسلطة الترخيص وغيرهما، إذ يتم تخزين المعاملات والقضايا وحفظها داخل الجهاز بحيث يمكن الرجوع إليها في أيّ وقت.

أمّا القانون الأردني فنصّ على[2] أنه "لا تسري أحكام قانون المعاملات الإلكترونية على العقود والمستندات والوثائق التي تنظم وفقًا لتشريعات خاصة بشكل معيّن أو تتم بإجراءات محددة ومنها إنشاء الوصية وتعديلها، وإنشاء الوقف وتعديل شروطه، ومعاملات التصرف بالأموال غير المنقولة بما في ذلك الوكالات المتعلقة بها وسندات ملكيتها وإنشاء الحقوق العينية عليها باستثناء عقود الإيجار الخاصة بهذه

---

1 إيناس الخالدي، مرجع سابق، ص28.

2 المادة (6) من قانون المعاملات الإلكترونية الأردني.

الأموال، والوكالات والمعاملات المتعلّقة بالأحوال الشخصية، والإشعارات المتعلّقة بإلغاء أو فسخ عقود خدمات المياه والكهرباء والتأمين الصحي والتأمين على الحياة، ولوائح الدعاوى والمرافعات وإشعارات التبليغ القضائية وقرارات المحاكم، والأوراق المالية إلا ما تنصّت عليه تعليمات خاصة تصدر عن الجهات المختصة استنادًا لقانون الأوراق المالية النافذ المفعول".

يلاحظ من هذا النص أنّ المشرع الأردني استثنى بعض المعاملات من إطار وسائل التكنولوجيا الحديثة بنص صريح حتى لو كانت مستوفية لكافة الشروط والأوضاع القانونية التي نص عليها القانون، أيضًا المشرع ذكر هذه المعاملات على سبيل المثال لا الحصر، فقد أورد المشرع هذه الاستثناءات نظرًا لأنها تمس حقوق الأفراد بشكل عام ولا تتعلق بعلاقات فردية، فالشخص الذي يقوم بإنشاء وصية ثم بعد ذلك توفي فلا يمكن بأي حال من الأحوال أن يتمكّن من التوصل إلى معرفة مدى صحة توقيعه الإلكتروني الوارد على السند الإلكتروني كونه توفي، وبخاصة أنه يمكن استخدام أكثر من نوع من أنواع التوقيع الإلكتروني إضافة لخطورة مثل هذه المعاملات من الناحية العملية، وكذلك الأمر بالنسبة للوقف[1].

إنّ هذه المعاملات تتعلق بشريحة واسعة من أفراد المجتمع كبيع الأموال المنقولة أو الوكالات العامة أو الخاصة، وكذلك الأمر بالنسبة لعقود اشتراك المياه والكهرباء وغيرها، وبالتالي ولأهمية مثل هذه المعاملات وخطورتها قام المشرع باستثنائها من تطبيق القانون عليها، وبالتالي عدم إمكانية استخدام الوسائل الإلكترونية لإنشائها أو تعديلها أو إثباتها، كما هو حال الكثير من تشريعات الدول الأخرى كحال المشرع

---

1 تنص المادة (1237) من القانون المدني الأردني على أنه "يتم الوقف أو التغير في مصارفه وشروطه بإشهار رسمي لدى المحكمة المختصة وفقًا للأحكام الشرعية".

بإمارة دبي الذي استثنى بعض هذه الأوضاع القانونية من قانون تطبيق المعاملات عليها، أمّا المشرع الفرنسي فقد تجاوز ذلك واعتبر أن الكتابة الإلكترونية يمكن اعتمادها في إبرام التصرفات القانونية التي تشترط فيها الشكلية كبيع الأرض أو السيارة[1].

ويرى البعض أن~ المشرع الأردني قد استثنى هذه المعاملات من تطبيق أحكام قانون المعاملات الإلكترونية عليها مؤقّتًا، أو ما لم يرد نصّ خاص بحقّها ومبرّرًا ذلك بأنّ الاتجاه إلى مشروع الحكومة الإلكترونية يشير إلى ذلك إشارة واضحة؛ أي: أنه من الممكن قبول إجراء مثل هذه المعاملات وغيرها بشكل إلكتروني في المستقبل، لافتًا أنه لا بد من قيام الحكومة باتباع إجراءات محدّدة حتى تتم عملية إجراء المعاملة بطريقة إلكترونية، وذلك بإيضاح إليه إجراء مثل هذه المعاملة، والشكل الذي تتم به، وطريقة إجراء مثل هذه المعاملات، ونوع التوقيع الإلكتروني المطلوب، وطريقة توثيقه لإثباته، وإجراءات الرقابة لغايات تعديل نصوصه[2] .

ولقد عمدت معظم التشريعات الأجنبية إلى إخراج بعض أصناف المعاملات في نطاق استخدام التوقيع الإلكتروني، مركّزة في ذلك على التصرّفات التي تستوجب الشكلية الخاصة لإتمامها، بالإضافة إلى معاملات الأوراق المالية.

إذ نجد أنّ القانون الفيدرالي للولايات المتحدة الأمريكية الخاص بالتوقيع الإلكتروني في مجال التجارة العالمية والقومية الصادر في 2000م جاء فيه أن هذا

---

1 يوسف أحمد النوافلة، مرجع سابق، ص 101 وما بعدها.

2 عبد الفتاح بيومي حجازي، مقدمة في التجارة العربية الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، 2003م، ص 62 وما بعدها.

القانون، لا يطبق في إنشاء وتنفيذ الوصايا وشهادات منح الثقـــة والتبنـــي والطـــلاق والأمور المتعلقة بالأسرة، نزع الحيازة وإنهاء الرهون.

أمّا التوجيه الأوروبي الصادر في 1999/12/13م فقد قرّر عدم تطبيق التوقيع الإلكتروني على العقود المنشئة والناقلة لحقوق عقارية فيما عـــدا حقـــوق الإيجـــار، والعقود التي تتطلب تدخّلاً من المحاكم والسلطات العامة، وعقود الكفالة والعقود التي يحكمها قانون الأسرة أو قانون الميراث مثل الوصية، الهبـــة، الطـــلاق، الـــزواج، التبني[1].

أمّا بالنسبة لقانون الأونسيترال النموذجي بخصوص التجارة الإلكترونيـــة فإنـــه يطبق فقط على المعاملات التجارية تحديدًا، وهذا من يستنبط من خـــلال مـــا نـــصّ عليه[2] "ينطبق هذا القانون على أيّ نوع من المعاملات يكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية".

---

1 خالد ممدوح إبراهيم، الشكلية في عقود الإنترنت والتجارة الإلكترونية، منشور على الموقع الإلكتروني، تاريخ الاطلاع عليه: 20 -2-2017م.

http://kenanaonline.com/users/KhaledMamdouh/posts/77862

2 المادة (1) من قانون الأونسيترال النموذجي بخصوص التجارة الإلكترونية.

المبحث الثاني
آثار التوقيع الإلكتروني وتطبيقاته

تمهيد وتقسيم:

يترتّب على الأخذ بنظام التوقيع الإلكتروني آثار مهمّة على التعاملات والتصرفات القانونية، التي يكون طرفها الأفراد أو المؤسسات الخاصة أو العامة، إذ سيكون بمقدور المستهلك ورجال الأعمال والسلطات العامة في الدولة، أن يدخلوا في اتفاقات تعاقدية وفي إجراء تعاملاتهم باستخدام التوقيع الإلكتروني، كما لو كانوا يستخدمون المستندات الورقية والتوقيعات المحررة بخط اليد، وسوف نتناول في هذا المبحث الآثار المترتبة على توافر شروط حجية التوقيع الإلكتروني وتطبيقاته من خلال المطلبين الآتيين:

المطلب الأول: آثار التوقيع الإلكتروني

المطلب الثاني: تطبيقات التوقيع الإلكتروني

المطلب الأول: آثار التوقيع الإلكتروني

نتيجةً لازدياد التعامل بالوسائل الحديثة لتقنيات التوقيع الإلكتروني كبديل للتوقيع التقليدي، ظهرت الحاجة إلى إيجاد إطار قانوني يهدف إلى الحدّ من عدم اليقين في الأثر القانوني الذي ينتج عن استخدام هذه التقنيات، والذي يتطلب إيجاد نصوص قانونية موحّدة تتعامل مع هذه التقنيات الحديثة. وفي غالبية القوانين المقارنة نجد أنه توجد نصوص خاصة تعطي التوقيع الإلكتروني حجية تعادل ما يتمتّع به التوقيع

التقليدي، حيث اعتبرت هذه النصوص أن وجود التوقيع الإلكتروني على محرّر يشترط فيه القانون التوقيع يفي بالغرض ويضفي على هذا المحرر أو المستند كامل الحجية التي يتطلبها ويشترطها المشرع[1].

في ضوء اعتراف المشرع بحجية التوقيع الإلكتروني في الإثبات، فإنّ سلطة القاضي التقديرية قد تقلّصت والتزم بالأخذ بالمحررات الإلكترونية وبالتوقيع الإلكتروني كدليل إثبات له كامل الحجية متى ما توافرت شروطه المتطلبة قانونًا.

ومن هنا ظهرت الحاجة إلى تقنين قواعد تكفل للتوقيع الإلكتروني حجيته شريطة توافر الشروط التي تطلبها المشرع فيه.

وقد نصّ نظام التعاملات الإلكتروني السعودي على أنه[2] "يكون للتعاملات والسجلات والتوقيعات الإلكترونية حجيتها الملزمة، ولا يجوز نفي صحّتها أو قابليتها للتنفيذ، ولا منع تنفيذها بسبب أنها تمّت –كليًّا أو جزئيًّا– بشكل إلكتروني، بشرط أن تتم تلك التعاملات والسجلات والتوقيعات الإلكترونية بحسب الشروط المنصوص عليها في هذا النظام".

كما نصّت الفقرة (2) من المادة ذاتها على أنه ((لا تفقد المعلومات التي تنتج من التعامل الإلكتروني حجيتها أو قابليتها للتنفيذ، متى كان الاطلاع على تفاصيلها متاحًا

---

1 عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني، مرجع سابق، ص 444، انظر أيضًا: عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة المكتب الجامعي الحديث، الإسكندرية، 2009م، ص 40 وما بعدها، انظر أيضًا: لورنس محمد عبيدات، مرجع سابق. ص154 وما بعدها.

2 الفقرة (1) من المادة (5) من نظام التعاملات الإلكتروني السعودي.

ضمن منظومة البيانات الإلكترونية الخاصة بمنشئها، وأُشير إلى كيفية الاطلاع عليها)).

لذلك فإنّ التوقيع الإلكتروني إذا ورد على محرّر إلكتروني فإنّ هذا المحرر له كامل الحجية في الإثبات، ما دام التوقيع محقّقًا للشروط التي حددها المشرع من حيث ارتباطه بشخصية مصدره، وتعبيره عن هويته، والذي يسمح للطرف الثاني تحديد هوية مصدره، كما أنّ المشرع أوجب أن يصدر الموقِّع توقيعه أثناء سريان شهادة التوثيق لكي يتمتّع بالحجية القانونية، وأوجب المشرع صفة الاستمرارية في استخدام التوقيع الإلكتروني بحيث لا يتمكّن الموقِّع أو الغير من إحداث أيّ تغيير أو تعديل على التوقيع[1].

وإذا ما كان التوقيع الإلكتروني قد تمّ توثيقه بصورة كاملة، واستوفى كافة المتطلّبات التي يشترطها القانون لإضفاء الحجية القانونية عليه، وبالاعتراف بقدرته على أداء وظائف التوقيع التقليدي، والمساواة بينهما، فهو بذلك منتج للآثار المترتبة على التوقيع التقليدي ذاتها من حيث إلزامه لأصحابه، وقيمته في الإثبات.

الفرع الأول: إلزام التوقيع الإلكتروني لصاحبه

باعتبار أنه بمجرد وضع التوقيع على أية ورقة أو سجل أو محرر، سواء كان هذا التوقيع إمضاء أم ختما أم بصمة، يجعل صاحبه ملزمًا بما ورد في الورقة أو السجل أو المحرر من حقوق والتزامات.

---

1 لورنس محمد عبيدات، مرجع سابق، ص 156 وما بعدها.

فالذي يعطي القيمة القانونية للكتابة العرفية هو التوقيع عليها، كذلك الحال في المعاملات الإلكترونية، لذا فإنّ وجود التوقيع على السجل الإلكتروني يلزم صاحبه بما ورد في السجل الإلكتروني[1].

غير أنه وباعتبار أن التوقيع الإلكتروني ليس له حجية، إلا إذا كان موثقًا والتوثيق يتم عن طريق إجراءات توثيق محدّدة بنص القانون، فالأمر في المعاملات الإلكترونية يختلف عنه في السند العادي إذا ما أنكر الموقع توقيعه، إذ يكون من الصعب على من نسب إليه توقيع إلكتروني أن ينكر صدور هذا التوقيع عنه ما دام التوقيع يتطابق مع رمز التعريف الموجود في الشهادة الإلكترونية، التي تعتبر بمثابة الهوية الإلكترونية للشخص ولا تتم المعاملة، إلا بعد التأكّد من شخصية صاحب الشهادة[2].

الفرع الثاني: القيمة القانونية للتوقيع الإلكتروني في الإثبات

إنّ معظم التشريعات المنظّمة للتوقيع الإلكتروني أو للمعاملات الإلكترونية، اعتبرت أنّ التوقيع الإلكتروني صالحًا للإثبات تمامًا كما هو الحال في التوقيع التقليدي، وألغي كلّ تمييز فيما بينهما، وذلك متى كان التوقيع الإلكتروني مستوفيًا لجميع شروطه القانونية واستخدم في حدود نطاق قبوله، فله الأثر القانوني نفسه الذي هو للتوقيع التقليدي، وبالنظر إلى وظائف التوقيع الإلكتروني نجد أن له القدرة على إثبات كافة المعاملات القانونية إذا ما استخدم ضمن الضوابط والشروط التقنية، كونه

1 علاء محمد نصيرات، مرجع سابق، ص148.

2 علاء محمد نصيرات، مرجع سابق، ص148.

يحدّد هوية الشخص الموقع ويعبر عن إرادته في الموافقة علـــى مضـــمون الســـند الإلكتروني، ويثبت سلامة المحرر الإلكتروني بامتياز.

بذلك يصلح التوقيع الإلكتروني لإثبات جميع المعـــاملات التـــي تـــتم بوســـائل إلكترونية مهما كانت طبيعة هذه المعاملة ومهما كانت قيمتها، إلا تلك التي يتطلـــب القانون لإتمامها شكلية معينة أو إجراءات محددة.

كلّ ذلك بشرط أن يكون التوقيع الإلكتروني متّفقًا مع أحكام القانون، من حيـــث التوثيق ووجود شهادة التوثيق، وتطابق التوقيع الإلكترونـــي مـــع رمـــز التعريـــف الموجود في شهادة التوثيق وغيرها من الشروط التي يتطلّبها القـــانون لكـــي يكـــون التوقيع الإلكتروني صالحًا للإثبات[1].

وإذا تحقّقت الشروط السابقة الذكر في التوقيع الإلكتروني والكتابة الإلكترونية والمحررات والمستندات الإلكترونية، فإنّها تتمتّع بالحجية الكاملة في الإثبات أمام جميع الجهات الرسمية في الدولة، وكذلك أمام القضاء كدليل إثبات كامل. ويتعيّن على القاضي الأخذ بالتوقيع الإلكتروني كحجة كاملة في الإثبات شريطة أن يتبيّن له صحته[2].

وفي حالة ما إذا كان المحرّر الإلكتروني متساويًا مع المحرر الكتابي من حيث استيفاء كلّ منهما شروط اعتباره دليلاً كتابيًّا كاملاً، وكان مضمون أحدهما متعارضًا

1 علاء محمد نصيرات، مرجع سابق، ص151 /152.

2 عبد الفتاح حجازي، النظام القانوني للتوقيع الإلكتروني، مرجع سابق، ص 443. انظر أيضًا: ثروت عبد الحميد، التوقيع الإلكتروني، مرجع سابق، ص 100 وما بعدها. انظر أيضا: ممدوح محمد علي مبروك "مدى حجية التوقيع الإلكتروني في الإثبات"، دار النهضة العربيةــ القاهرة، 2005م، ص 174 وما بعدها.

مع الآخر، فإنّ التنازع بينهما يحدث، وعلى قاضي الموضوع أن يأخذ بالمحرر الذي يطمئن إليه أيًّا كانت طريقة تدوينه، وسواء كان إلكترونيًّا أم كتابيًّا، ما دام لم يوجد نص قانوني أو اتفاق بين الأطراف في العقد يعيّن أسسًا أخرى للترجيح بين الأدلة في حالة الاختلاف[1].

المطلب الثاني: تطبيقات التوقيع الإلكتروني

نظرًا لما يحظى به التوقيع الإلكتروني من مزايا، كفلت له انتشارًا واسعًا وتزايدًا مستمرًّا في الاستخدام، وذلك في مجالات عدة، سواء على مستوى المعاملات القانونية بين الأفراد أم المؤسسات، وإنّ من أهم تطبيقاته نجد البطاقات البلاستيكية، التلكس، الشيك الإلكتروني وسند الشحن الإلكتروني وغيرهم، سنقتصر في دراستنا على عرض استخدام التوقيع الإلكتروني في البطاقات البلاستيكية، ثم التلكس.

الفرع الأول: البطاقات البلاستيكية

اخترنا البطاقات البلاستيكية كدراسة تطبيقية، لانتشار استخدامها في البنوك وفي المعاملات التجارية عبر الإنترنت، وقد ظهرت أخيرًا في البريد لتحلّ محلّ الشيك الورقي، ويمكن القيام بعمليات أخرى مثل الاطلاع على الرصيد، والسحب والتحويل. وسنحاول التطرق لأنواعها ثم التوقيع الإلكتروني فيها، ومدى حجيته في النقاط الآتية:

---

1 أسامة بن غانم العبيدي، حجية التوقيع الإلكتروني في الإثبات، منشور على الموقع الإلكتروني، www.nauss.edu.sa/Ar/CollegesAndCenters/.../1434/.../em،dar،56،4.pdf، تم الاطلاع عليه بتاريخ: 14/02-2017م.

أنواع البطاقات البلاستيكية:

أ. البطاقات الائتمانية (المصرفية) Credit Card:

عرفها مجمع الفقه الإسلامي الدولي بأنها مستند إلكتروني، يعطيه مصدره لشخص طبيعي أو اعتباري بناء على عقد بينهما، يمكنه من شراء السلع والخدمات ممن يعتمد المستند دون دفع الثمن حالاً، لتضمنه التزام المصدر بالدفع، ومنها ما يمكن من سحب النقود من المصارف[1].

فهي بطاقة بلاستيكية يمنحها المصدر للحامل، ويمنح له خط ائتمان، فيستطيع من خلالها شراء مستلزماته ثم التسديد لاحقًا، وإذ لم يستطع التسديد في أيّ شهر يسمح له بتدوير جزء أو كل المبلغ، مقابل دفع فائدة على رصيد المدين القائم، ويمكن استخدمها للدفع عبر الإنترنت[2].

ب. بطاقة الحساب "Charge Card":

وهي بطاقة تتيح للمستهلك الشراء على الحساب والتسديد لاحقًا، ولا بد على حاملها تسديد المبلغ بكامله، عندما يرسل المصدر فاتورة له، ولا يتحمل المستهلك جراء ذلك أية فوائد[3].

---

1 فيصل سعيد الغريب، مرجع سابق، ص 239.

2 علاء محمد نصيرات، مرجع سابق، ص 42.

3 علاء محمد نصيرات، مرجع سابق، ص 42.

ج. البطاقة المدينة (بطاقة الوفاء debted card):

تسمح هذه البطاقة لحاملها بتسديد مشترياته من خلال السحب على حسابه الجاري في المصرف مباشرة، فالعميل عند العمليات المختلفة، من سحب النقد، ودفع قيمة المشتريات يحوّل الأموال العائدة له إلى حساب البائع التاجر مباشرة، فإذا كانت البطاقة "On- line" على الخط يتم تحويل الأموال يوميًّا، أمّا إن كانت خارج الخط "Of -line" فإنّ التحويل يتم خلال عدة أيام لاحقة.

د. بطاقة الصراف الآلي "A.T.M":

تسمح هذه البطاقة بالدخول إلى مكنونات المصرف المؤتمنة، وإلى الشبكات المرتبطة بها العائدة للمصارف الأخرى، ويستطيع العميل إجراء العديد من المعاملات المصرفية النمطية، مثل التحويل من حساب لآخر، إيداع وسحب الأموال، وتسديد بعض الفواتير[1].

ه. البطاقة الذكية "Smart Card":

تعتبر هذه من أهم أنواع البطاقات، كونها تحتوي على شريحة ذكية تسمى ميكرو بروسيسور "Microprocessor puce"، ممّا يجعلها عبارة عن كومبيوتر مصغر لا يزيد حجمه عن الظفر، ويمكن طبع برمجته لتلبية بعض الوظائف بواسطة شركات مختصّة، فتدخل بعض المعلومات في الذاكرة، مثل اسم صاحب البطاقة، مؤسسة العمل الجهة المصدرة للبطاقة، تاريخ سريانها، ثم تبرمج دالة جبرية أو

---

1 فيصل سعيد الغريب، مرجع سابق، ص 236.

خوارزمية مسؤولة عن توليد الرقم السري، وعند كلّ استعمال يدخل العميل البطاقة في آلة قراءة مع إدخال الرقم السري المولد في البطاقة، فإذا كانا متطابقين تتم العملية المزمع القيام بها، وإذا كانا غير متطابقين يعطى حامل البطاقة محاولتين أخريين، فإذا أخطأ رغم هذا في إدخال رقم سري صحيح يطلق "Microprocessor" أمرًا لإفساد وتعطيب نفسه[1].

التوقيع الإلكتروني في البطاقة البلاستيكية:

يجمع بين كلّ أنواع البطاقات البلاستيكية، اعتمادها على الرقم السري عند استخدامها للقيام بعمليات معينة، ويتم ذلك بسلك الخطوات التالية[2] إدخال البطاقة التي تحتوي على البيانات الخاصة بالعميل في جهاز مخصّص، وكتابة الرقم السري المخصص لصاحب البطاقة، وإصدار الأمر للقيام بالعملية المراد إتمامها بالضغط على المفتاح المخصّص، وبذلك يكتمل التعبير عن الإرادة في قبول إتمام العملية، فالرقم السري يستعمل لتعريف وتحديد هوية المتعامل أو الزبون، بالإضافة إلى توقيع العمليات الحسابية دون استعمال ورق، ويتم إثبات عملية السحب على ثلاثة أنواع من المخرجات: على شريط ورقي موجود خلف الجهاز، على أسطوانة ممغنطة، وفي حالة قيام نزاع بين البنك والعميل حول عملية السحب ذاتها، أو مقدار المبلغ الذي تم سحبه، فإنه يكفي للمؤسسة المصرفية تقديم تسجيل للعمليات التي تمّت بواسطة جهاز الحاسب الآلي.

1 علاء محمد نصيرات، مرجع سابق، ص 43.

2 علاء محمد نصيرات، مرجع سابق، ص44.

مدى تعارض التوقيع الإلكتروني في البطاقات البلاستيكية مع مبادئ الإثبات:

لمّا كان إثبات العملية أو مقدارها يتم بتقديم تسجيل للعمليات التي تمت بواسطة جهاز الحاسب الآلي، ولما كان هذا الجهاز يخضع لسيطرة المؤسسة المصرفية، ولها حرية التصرف فيه، فإنّه من المفروض ألا يعتدّ به، لأنه يتعارض مع مبدأ أساسي في الإثبات، وهو أنه لا يجوز للشخص أن يصطنع دليلاً لنفسه، ومع ذلك ميّزت محكمة النقض الفرنسية بين فرضين: حالة ما إذا كانت الأداة أو الجهاز المستمد منه التوقيع يخضع للسيطرة التامّة لمقدّم الدليل، أو أحد تابعيه في عمليتي التحضير والتشغيل، فترفض على ذلك الأساس الاستناد إلى هذا الدليل وتعتبره اصطناعًا للدليل لصالحه.

أمّا الفرض الثاني ألا يكون لمقدم الدليل أيّ سيطرة على المنظومة المعلوماتية المتعلقة بتسجيل العمليات الواقعة من طرف العميل[1]، فتقبله ولا تعتبره اصطناعًا للدليل.

فلا يوجد تعارض هنا بين التوقيع الإلكتروني في البطاقات البلاستيكية مع مبادئ الإثبات، ويمكن الاعتداد بما ورد في هذه الأجهزة لإثبات مختلف العمليات التي كانت قد أنجزها العميل، دون أن يكون ذلك اصطناع المؤسسة دليلاً لصالحها.

وبما أنّ الجهاز بمجرد وضعه في العمل يصبح أداؤه آليًّا، وذاتيًّا، ويقتصر دور المؤسسة على صيانة الجهاز، دون المساس بالنظام المسؤول على القيام بالتعرف على منشأ البطاقة، ومدى توافقها مع الجهاز ثم التعرف على العميل بمطابقة الرقم السري الذي يحمله مع قاعدة البيانات المرجعية، التي كونتها المؤسسة بمناسبة

1 ثروت عبد الحميد، مرجع سابق، ص 79-80.

طلبات الحصول على البطاقة، وذلك يعدّ بمثابة المرور على حاجز أمني، وفي حالة اجتيازه يمنح النظام مربع حوار لمجمل العمليات التي يمكن القيام بها عن طريق البطاقة، بالإضافة إلى أنّ الجهاز يقدّم مستخرجًا مكتوبًا على الورق يمنح للعميل بمجرد الانتهاء من العملية التي قام بها.

الفرع الثاني: التلكس

يعتبر التلكس من وسائل الاتصال الحديثة التي أصبحت تستخدم في عدة مجالات، ومنها إجراء الصفقات والعقود بين الأفراد والمؤسسات، فما هو التلكس وما حجيته في الإثبات؟

نحاول الإجابة في النقاط الآتية:

تعريف التلكس:

يعرّف التلكس بأنه جهاز إلكتروني مبرق متصل بدعامة يطبع البيانات الصادرة من المرسل بلون أحمر، والبيانات الصادرة من المرسل إليه باللون الأسود، ويستطيع المشترك الاتصال مباشرة مع أيّ مشترك آخر يملك الجهاز نفسه، لإرسال إيجابه وتلقي ردّه، فلكلّ مشترك رقم ورمز نداء من الجهاز المرسل إليه[1].

طريقة عمله:

يعمل التلكس عن طريق ما يسمى بالتشفير المتماثل، فهو يستخدم نظام "النداء الذاهب"، ويقصد به أن رمزًا معيّنًا يمكن أن ينتقل بين جهازين متّصلين ببعضهما بخط واحد، وبهذا الأسلوب نفسه يمكن استلام النداء الراجع من أحدهما، ويقوم جهاز

1 علاء محمد نصيرات، مرجع سابق، ص 51.

التلكس بتحويل الحروف المكتوبة التي تتم عن طريق الإرسال، والاستلام بالاتصال السلكي واللاسلكي، إلى نبضات كهربائية فيتحول الضغط على الحروف إلى إشارات كهربائية، تتحوّل إلى إشارات كهرومغناطيسية، تمرّ خلال أمواج ليقوم بتسلّمها جهاز التلكس الذي تنعكس فيه العملية إلى طبع الحرف المرسل[1].

استخدام التلكس في البنوك:

يحرّر البنك الآمر بالدفع برقية إلى بنك المستفيد، يطلب منه دفع مبلغ معين مع تحديد تاريخ التحرير واسم المستفيد، ثم يوقّعه بوضع عدد معروف بالمفتاح أو الشفرة، على زاوية في البرقية، وهو ناتج عن دالة رياضية تستند إلى قاعدة سرية لا يعرفها إلا البنك المرسل إليه، والبنك الباعث، وحتى داخلهما لا يعرفونها إلا الموظفين المخولين للإذن بتلك العمليات، يقوم البنك المراسل عند تلقي التلكس بحلّ المفتاح أو الشفرة حسب القاعدة المتبادلة، وبالسرية المتّفق عليها مع البنك العميل الآمر بالدفع، فإذا وجد العدد نفسه على البرقية أدرك أنها صادرة عن الآمر فينفذ العملية بكل أمان، أمّا إذا اختلف العددان فيرفض إنجاز العملية ويتصل بالبنك الآمر للتثبّت في أمر البرقية.

مميزات التلكس:

يتمتّع التلكس بالسرعة والسرية والوضوح، وأهمّ سمة له أنه يترك أثرًا ماديًّا مكتوبًا للوثائق المرسلة عن طريقه[2]، فهو بذلك يعتبر بيئة آمنة لتبادل الرسائل، وبخاصة أنه يستخدم في شبكة خاصة يتحكم في إدارتها، ومراقبتها شخص وسيط

---

1 ثروت عبد الحميد، مرجع سابق، ص 142.

2 علاء محمد نصيرات، مرجع سابق، ص 52.

محايد يقوم بدور شبيه لمكاتب البريد، فالوسيط يحدد هوية طرفي الرسالة، ويتحقّق من تلقي جهاز المرسل إليه للرسالة ويؤرّخ عملية الإرسال، ثم إنّ الوسيط يحتفظ بما يدلّ على تبادل الرسائل خلال مدة معيّنة، وهذه الإجراءات تكفل حدًّا أدنى من الأمان فيما يتعلّق بعمليتي الإرسال والاستقبال.

الاعتراف التشريعي بحجية التلكس:

لقد كانت حجية التلكس محلّ جدل بين الفقه من مؤيد ومعارض، وكانت معظم قوانين الإثبات لا تعطيه أية حجية إلا على سبيل الاستثناء[1]، لكن فيما بعد اعترفت به، ومن ضمنها المشرع الإماراتي حيث نصّ قانون الإثبات في المعاملات المدنية والتجارية الإماراتي على[2] أن "تكون للرسائل الموقّع عليها قيمة المحرر العرفي من حيث الإثبات، وتكون للبرقيات هذه القيمة أيضًا إذا كان أصلها المودع في مكتب التصدير موقّعًا من مرسلها، وتعتبر البرقية مطابقة لأصلها حتى يقوم الدليل على عكس ذلك. وإذا لم يوجد أصل البرقية، فلا يعتدّ بالبرقية إلا لمجرّد الاستئناس.

أمّا المشرع الجزائري في القانون المدني الذي نصّ على[3] أن "تكون للبرقيات هذه القيمة أيضًا (قيمة الأوراق العرفية) إذا كان أصلها المودع في مكتب التصدير موقعًا عليها من مراسلها، وتعتبر البرقية مطابقة لأصلها حتى يقوم الدليل على عكس ذلك، وإذا تلف أصل البرقية فلا تعتبر نسختها إلا لمجرد الاستئناس"، ونظام إرسال البرقيات هو نفسه النظام المستخدم في التلكس، ما عدا أنه في حالة التلكس تكون

---

1 علاء محمد نصيرات، مرجع سابق، ص 53.

2 المادة (14) من قانون الإثبات فى المعاملات المدنية والتجارية الإماراتي رقم 1992/10.

3 المادة (329) من القانون المدني الجزائري.

الرسالة مشفرة أمّا في البرق فلا، لأنّ أطراف التعامل يلجؤون إليها نظرًا للسرعة والأمان الذي يتمتع به.

ومن نصّ المادة المذكورة نجد أن المشرع الجزائري قد أعطى المحرّرات الناجمة عن التلكس القيمة ذاتها للمحررات الورقية، وافترض أنها مطابقة لأصلها المودع في مكتب التصدير حتى يقوم العكس، ويمكن الرجوع لمكاتب التصدير للتحقّق من قيام المرسل والمرسل إليه بالعملية موضوع النزاع، ولا بد أن يكون الأصل موقعًا عليه تحت طائلة عدم اعتباره دليلاً كتابيًّا كاملاً.

أمّا إن لم يكن أصل البرقية موجودًا لدى مكتب التصدير فإنّ مستخرج التلكس حتى إن كان ممهورًا بالتوقيع، وجميع البيانات الضرورية المحددة فإنه يكفي إنكار التوقيع ليفقد قيمته كمحرّر مكتوب.

وخلاصة القول إنه وعلى شاكلة اعتماد التوقيعات الإلكترونية على الأوراق البلاستيكية والتلكس وتنظيمها بشكل جيد، يمكن تنظيم مسألة التوقيع الإلكتروني من بابها الواسع وتنظيمها بشكل يمنع من وقوع الفوضى في التطبيق، وكذا التلاعبات المحتملة في حال ترك الباب مفتوحًا بمصراعيه.

المبحث الثالث

وظيفة التوقيع الإلكتروني ودوره في الإثبات

تمهيد وتقسيم:

أصبحت الحاجة ملحّة لاستخدام التوقيع الإلكتروني في عصر التكنولوجيا وتقنية المعلومات، فلم يعد التوقيع التقليدي كافيًا في عالم تسوده المعاملات الإلكترونية التي حلّت المستندات الإلكترونية فيها محلّ المستندات الورقية التقليدية، فما إن بدأت تقنيات الاتصال تتطور يومًا بعد يوم حتى أصبح من الضرورة العمل على مواكبة هذا التطور من خلال تطوير الوسائل المستخدمة في المعاملات المختلفة، وقد جاء التوقيع الإلكتروني ليتناسب مع تقنيات الاتصال الحديثة، ليؤدّي الدور الوظيفي نفسه الذي يقوم به التوقيع التقليدي مع اختلاف البيئة التي يتم فيها كلّ منهما. فالتوقيع الإلكتروني يتم بوسائل إلكترونية في بيئة إلكترونية تتم فيها المعاملات عن بعد بوساطة وسائل الاتصال الحديثة، فللتوقيع الإلكتروني دور في الإثبات لا يقلّ أهمية عن التوقيع العادي، وهذا ما سأتناوله في هذ المبحث: وظيفة التوقيع الإلكتروني ودوره في الإثبات من خلال المطلبين الآتيين:

المطلب الأول: وظيفة التوقيع الإلكتروني في الإثبات

المطلب الثاني: دور التوقيع الإلكتروني في الإثبات

المطلب الأول: وظيفة التوقيع الإلكتروني في الإثبات

تعود أزمة مسألة الإثبات في الحقيقة إلى التطور العلمي، ويعني ذلك أنّ الحقيقة العلمية قد أثرت في وسائل الإثبات المعتمدة سواء قانونًا أم اتّفاقًا فلم يعد ممكنًا أن يتجاهل رجال القانون الأبحاث والتطورات العلمية الفاعلة في العلاقات الاجتماعية، كما لم يعد مسموحًا أن ينكر القانون الإفرازات العلمية الحديثة، ولما كان نجاح القاعدة القانونية يقتضي مواكبة التطورات الحديثة، فإنّ القانون محمول على إعادة صياغة علاقته بالمقتضيات العلمية حتى يصبح العلم في علاقة تكاملية مع القانون.

إنّ التوقيع يعدّ عنصرًا مهمًّا وفعّالاً في المعاملات التجارية المحلية والدولية، فهو جزء من العقد أو المستند، ودون ذلك لا يكون للسند أيّة قيمة قانونية في الإثبات، ومع ازدياد التطور التكنولوجي وتطوّر المعاملات بين الأفراد اتّسع مفهوم التوقيع، فلم يعد قاصرًا على التوقيع التقليدي، فقط بل شمل أيضًا التوقيع الإلكتروني، وإنّ هذا التحوّل من استخدام التوقيع التقليدي إلى التوقيع الإلكتروني في مجال المعاملات المدنية والتجارية يوجب الحفاظ على الدور الذي يلعبه التوقيع التقليدي، وهذا ما سعى إليه فقهاء القانون والقضاء محاولة منهم في إيجاد نوع من الحماية للتوقيع الإلكتروني، وما نتج عن ذلك بين مؤيد ومعارض، فالرأي المعارض لا يفرق بين وظيفة التوقيع وشكله، ومن ثمّ لا يعتدّ به في الإثبات، أمّا الرأي المؤيّد والراجح فيفرّق بين وظيفة التوقيع وشكله، ومن ثمّ فإنّ التوقيع الإلكتروني من حيث وظيفته يمكن اعتباره حجة في الإثبات لقيامه بالوظائف نفسها التي يقوم بها التوقيع العادي، وهو تحديد هوية الموقع وإظهار موافقته على الالتزام بمضمون المحرّر

الذي قام بتوقيعه[1]. وهناك من يرى في هذا الموضوع أنه لا يوجد أيّ حجية لهذا النوع من التوقيع بسبب عدم توفر الأمان والضمانات الكافية واللازمة لمثل هذا التوقيع، إلا أنّه وبصدور القوانين الخاصة بالتجارة الإلكترونية أعطيت، الحجية لمثل هذا التوقيع، وذلك من خلال وضع إجراءات تحقّق الأمن والثقة به، وتوفّر له الحماية القانونية والتقنية، حيث يتم إصدار التوقيعات من قبل جهة معتمدة تصدر شهادات توثيق به ويكون مودعًا لديها[2]. وهي تعمل بترخيص وتحت إشراف السلطة التنفيذية، وتقوم هذه الجهة بتقديم شهادة إلكترونية لتأكيد هوية الموقع وصفته وصحة توقيعه ونسبة رسالة البيانات أو العقد لصاحبه[3]. وقد كان أوّل اعتراف بالتوقيع الإلكتروني عام 1989م في مجال البطاقات الائتمانية، حيث أقرّت محكمة النقض الفرنسية بصحة التوقيع الإلكتروني، واعتبرت أنه يتألّف من عنصرين، هما: إبراز البطاقة الائتمانية، وإدخال رقم حامل البطاقة السري. وأكّدت هذه المحكمة كذلك أنّ هذه الوسيلة توفّر الضمانات الموجودة في التوقيع اليدوي، بل تفوقها[4].

وبهذا الصدد نصّ قانون المعاملات والتجارة الإلكترونية لإمارة دبي على أنه[5] "يعامل التوقيع على أنه توقيع إلكتروني محميّ إذا كان من الممكن التحقّق من خلال

---

1 عبد العزيز المرسى حمود، مرجع سابق، ص 50.

2 حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2000م، ص 45.

3 محمد حسين منصور، المسؤولية الإلكترونية، دراسة مقارنة، الإسكندرية، دار الجامعة، 2003م، ص 281.

4 برهم، نضال إسماعيل، أحكام عقود التجارة الإلكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2005م، ص 177.

5 المادة (20) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي.

تطبيق إجراءات توثيق مُحكمة منصوص عليها في هذا القانون أو معقولة تجاريًا ومتّفق عليها بين الطرفين".

وقد أعطى قانون المعاملات والتجارة الإلكترونية لإمارة دبي في الفقرة (3) من المادة (12) منه كامل الحجية للتوقيع الإلكتروني التي يتمتّع بها التوقيع التقليدي، ومن مظاهر الحجية التي أسبغها هذا القانون على التوقيع الإلكتروني إمكانية التعديل عليه في جميع المعاملات والتصرفات القانونية، ويفترض هذا القانون أن صاحب التوقيع الإلكتروني وضع توقيعه بنية توقيع الرسالة؛ أي: أنّ نيته وإرادته اتجهت نحو سريان موضوع الرسالة أو التصرف القانوني في حقّه، وبالتالي تحمل كافة الالتزامات والحقوق الناتجة عن ذلك[1].

ونصّ قانون المعاملات الإلكترونية الأردني الأردني على[2] أنه "إذا استوجب تشريع نافذ توقيعًا على المستند أو نصّ على ترتيب أثر على خلوّه من التوقيع فإنّ التوقيع الإلكتروني على السجل الإلكتروني يفي بمتطلبات ذلك التشريع".

ونصّ قانون التوقيع الإلكتروني المصري[3] على أن "للتوقيع الإلكتروني، في نطاق المعاملات التجارية والمدنية والإدارية، ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية إذا روعي في إنشائه وإتمامه

1 انظر: محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، مرجع سابق، ص245 وما بعدها، انظر أيضًا: فيصل الغريب، التوقيع الإلكرتوني وحجيته في الإثبات، مرجع سابق. ص 255 وما بعدها.

2 المادة (10/ أ) من قانون المعاملات الإلكترونية الأردني.

3 المادة (14) من قانون التوقيع الإلكتروني المصري.

الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحدّدها اللائحة التنفيذية لهذا القانون".

نخلص ممّا سبق أنّ وسيلة الإثبات الإلكتروني لا تطبّق إلا على ما تم الاتفاق عليه فقط، أمّا ما سيتم الاتفاق عليه لاحقًا فهو شأن آخر لا يسري عليه الاتفاق السابق، وقد قصد المنظم من ذلك حث الأفراد المتعاملين للجوء للوسائل الإلكترونية في تنفيذ معاملاتهم دون أن يقوم بإجبارهم على ذلك(1).

ومن الملاحظ أنّ ما يسري بشأن القاعدة العامة في هذا الصدد يسري بشأن المعاملات الإلكترونية أيضًا، إذ إنّ الإثبات بهذه الوسيلة هو إثبات ناشئ عن الاتفاق ما بين الطرفين على إثبات معاملات محدّدة بينهم بالوسائل الإلكترونية، وبالتالي، تعتبر هذه الوسائل دليل إثبات كامل للمعاملات التي تتم بين الطرفين، وهذا ما أكدته المادة (5) من النظام ذاته، والتي أعطت المحررات الإلكترونية ذات حجية المحررات الخطية والتوقيع الخطي(2) .

ويلاحظ من النصوص السابقة أنّ المشرع المصري قد ساوى في الحجية ما بين التوقيع التقليدي والتوقيع الإلكتروني، وبذلك يمكن القول إنّ التوقيع الإلكتروني في ظل ضمانات معينة يمكنه أن يقوم بذات الدور الذي يؤديه التوقيع التقليدي، بل يرى

---

1 يحيى يوسف فلاح حسن، مرجع سابق، ص99 .

2 تنصّ المادة (15) من قانون التوقيع الإلكتروني المصري على أنه": للكتابة الإلكترونية والمحررات الإلكترونية، في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد التجارية والمدنية، متى استوفت الشروط المنصوص عليها في هذا القانون وفقًا للضوابط الفنية والتقنية التي تحدّدها اللائحة التنفيذية لهذا القانون."

البعض أن التوقيع التقليدي قد لا يجد له مكاناً في ظل المعالجة الإلكترونية للمعلومات، وبذلك يمكن الاعتماد على الرقم السري كوسيلة بديلة أو إضافية للتوقيع التقليدي، يمكنها أن تقوم بذات الدور التقليدي، فضلاً عن ملاءمتها لنظم المعلوماتية[1].

ولقد دخل توجيه التجارة الإلكترونية الخاصة بالاتحاد الأوروبي (EUE- Directive Commerce) حيّز التنفيذ في 17 يوليو من عام 2000م، وأصبح منذ نفاذة لازمًا على الدول الأعضاء في الاتحاد الأوروبي أن تطبّقه بحلول 17 يناير من عام 2002م. وقد كان الهدف من إصداره هو ضمان حرية حركة المعلومات والخدمات المعلوماتية. وتنشيط حركة التجارة الإلكترونية ونموّها بين الدول الأعضاء[2].

وبموجب هذا التوجيه فإنّه يجب على الدول الأعضاء الاعتراف بالصفة القانونية ونفاذية العقود الإلكترونية، وتفادي وضع قيود على استخدام مثل تلك العقود، إلا أنّ هذا التوجيه يعدّ إجرائيًّا وليس موضوعيًّا، ومن ثمّ لا يضع قواعد جوهرية في القانون الدولي.

ويوجب هذا التوجيه في المادة (5) منه على المنشأة التي تتعامل إلكترونيًّا أن تعلم عملاءها باسمها ومكان وجودها وعنوانها الإلكتروني. ولا يطبّق هذا التوجيه على التعاملات الضريبية والتعاملات المتعلّقة بكتابات العدل وحماية البيانات وحقوق الملكية الفكرية[3].

---

1 عبد الفتاح بيومي حجازي، مرجع سابق، ص 3.

2 European Council Directive 2000/31/EC, 2000 O.J. (L .178) 1-12 See

3 Article (5) , Council Directive , Id. at 8.

ويجوز للدول الأعضاء النص في قوانينها الوطنية على عدم تطبيق هذا في التعاملات العقارية والمسائل المتعلّقة بقانون الأسرة وأوراق المحاكم والوعود المتعلقة بدفع ديون الغير.

كما صدر توجيه التوقيع الإلكتروني الخاص بالاتحاد الأوروبي في عام 1998م، حيث بدأت عدة دول أوروبية في إصدار تشريعات تتعلّق بالتوقيع الإلكتروني المستخدم في التعاملات التجارية[1].

وقد خشي الاتحاد الأوروبي من وجود فروقات واختلافات بين تلك القوانين والتشريعات بل سعى إلى إيجاد أساس موحّد للوصول إلى توحيد تلك التشريعات. لذلك أصدر الاتحاد الأوروبي التوجيه الخاص بالتوقيع الإلكتروني للوصول إلى هذه الغاية.

وأوجب الاتحاد الأوروبي على جميع الدول الأعضاء تطبيق هذا التوجيه بحلول 19 يوليو من عام 2001 م.

وينصّ هذا التوجيه على وجوب الاعتراف بالحجية القانونية للتوقيع الإلكتروني والجوانب الدولية لهذا التوقيع[2]، كما ذكر التوجيه الأوروبي مستويين للتوقيع الإلكتروني: في المستوى الأول، يعرف بالتوقيع الإلكتروني البسيط. وهذا التوقيع وفقًا للمادة (2) من هذا التوجيه يعرّف بأنه: ((معلومة تأخذ شكلاً إلكترونيًا وترتبط بشكل منطقي ببيانات أخرى إلكترونية، والذي يشكّل أساس التوثيق)).

1 Anthony, Burke, EU and Irish Internet Law An Overview, 13 Int'l L. Practicum, at 107, 113 15 (Autumn 2000)

2 Jacqueline, Klosek (2000): EU Telecom Ministers Approve Electronic Signatures .Directive, 4 Cyberspace Law 12.

أمّا المستوى الثاني فهو التوقيع الإلكتروني المتقدم، وهو يعرف بأنه توقيع يتطلب صلة منفردة بالموقّع[1]، وأن يتيح كشف هوية الموقِّع، وأن يتم إنشاؤه باستخدام وسائل تحت رقابة الموقع، وأن يرتبط بالبيانات التي وضع عليها التوقيع بحيث إنّ أيّ تعديل لاحق على البيانات يمكن كشفه من قبل المتلقي[2]، كما عرّف هذا التوجيه شهادة التصديق الإلكتروني الصادرة عن مقدّم خدمات التوثيق الإلكتروني بأنها ((الشهادات الصادرة من جهات التوثيق المرخّص لها من قبل الجهات المختصة في الدولة)) لتشهد بأنّ التوقيع الإلكتروني هو توقيع صحيح يمكن نسبته إلى من أصدره، ويستوفي الشروط والضوابط المتطلبة فيه باعتباره دليل إثبات يمكن الاستناد إليه[3]، كما أكّد التوجيه الأوروبي أهمية دور مقدّمي خدمات التوثيق الإلكتروني في الحفاظ على المستوى المقبول من الحماية والأمان للتوقيع الإلكتروني والتعاملات الإلكترونية. ومن ثمّ تقوم مسؤولية مقدّم خدمات التوثيق الإلكتروني عن الأضرار التي تصيب أيّ جهة أو شخص يعتمد على شهادة تصديق إلكتروني[4].

ولم يتطلّب التوجيه الإلكتروني صراحة استعمال أيّة وسيلة تقنية معينة، ومن ثم فهو محايد من الناحية التقنية. ولكن التوجيه يؤكّد ضمنيًّا ضرورة استعمال أنظمة تقنية أمنية معقّدة لتحقيق أعلى درجات الحماية والأمان للتوقيع الإلكتروني والتعاملات الإلكترونية[5].

---

1 Council Directive 1999/93/FC , 2000/31/EC, 2000 O.J. (L .178) 1-12
2 I.d. at 10 , art . 13.
3 Id..at 11, Annex 11 (d) See also Council Derective , Supra, at 7 , art. 4 (2).
4 Council Detective , art . 4 (3) art.6.
5 Klosek, Jacqueline, EU Telecom Ministers Approve Electronic Signatures Supra. 12. Directive ,

ولقد تعاملت الأمم المتحدة مع التوقيع الإلكتروني من خلال قانونين، هما: القانون النموذجي للتوقيع الإلكتروني والقانون النموذجي للتجارة الإلكترونية الأونسيترال (UNCITRA)، وتم وضع هذا القانون من قبل لجنة الأمم المتحدة لقانون التجارة الدولية والمعروفة باسم الأونسيترال (UNCITRA) وتمت المصادقة عليه من قبل الجمعية العامة للأمم المتحدة في عام 1996م. ويهدف هذا القانون إلى إيجاد إجراءات ومبادئ لتسهيل استخدام التقنية الحديثة في تسجيل وإرسال المعلومات[1].

وتعطي المادة (7) من هذا القانون التوقيع الإلكتروني ذات الحجية القانونية الممنوحة للتوقيع التقليدي. واشترطت المادة توافر الشروط الآتية:

1. إمكانية تحديد هوية الموقِّع وموافقته على المعلومات الواردة في السجل.
2. أن تكون الطريقة المستخدمة لتحديد هوية الموقِّع موثوقة ويمكن الاعتماد عليها[2].

والملاحظ أنّ نصّ المادة (1) من قانون الأونسيترال النموذجي لم يتم تحديد معنى التجارة الإلكترونية، لذا فإنّه من الممكن أن مفهوم أنشطة تجارية قد يشمل في ظروف معينة استخدام تقنيات مثّل التلكس والنسخ البرقي، لذا ينبغي تفسيرها تفسيرًا واسعًا على أن يشمل المسائل الناشئة عن جميع العلاقات ذات الطابع التجاري سواء

---

1 United National Commission on International Trade Law, UNC, ITRAL Law on Electronic Commerce With Guide to Enactment (1996) , at http: // www.uncitral.org/ English / texts / telecom / ml. htm.

2 Id. at 6, art 7.

كانت تعاقدية أم غير تعاقدية، كالأعمال الهندسية والخدمات الاستشارية والتمثيل التجاري واتفاق التوزيع وغيرها من العلاقات التجارية[1].

ومن الملاحظ كذلك أنّ قانون الأونسيترال النموذجي تناول التجارة الإلكترونية في مجالات محدّدة من حيث تطبيقها على البضائع فقط، أمّا الجوانب الأخرى من التجارة الإلكترونية فقد تدعو الحاجة إلى تناولها في المستقبل، ومن ثمّ يمكن النظر إلى هذا القانون على أنه صكّ مفتوح المجال يكمل بأعمال ينظر بها مستقبلاً، فقد يتم تقرير أحكام جديدة أو تعديل الأحكام الحاليه وفقًا للظروف ومقتضيات المصلحة العامة[2] .

ولقد قامت لجنة الأمم المتحدة لقانون التجارة الدولية (الأونسيترال) بتكملة المادة (7) من القانون النموذجي للتجارة الإلكترونية بما أصبح يعرف بالقانون النموذجي للتوقيع الإلكتروني. وحسب نص المادة (2) من القانون النموذجي للتوقيع الإلكتروني، يقصد بالتوقيع الإلكتروني: ((بيانات إلكترونية مدرجة برسالة ومرتبطة بها منطقيًا، ويمكن استخدامها لتحديد هوية الموقِّع، وبيان موافقته على البيانات والمعلومات الواردة في الرسالة))[3].

---

1 عمر يونس، قانون اليونسترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996 م، المؤتمر الدولي الأول لقانون الإنترنت، ورشة عمل نحو علاقات قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة، المنظمة العربية للتنمية الإدارية، منظمة الدول العربية، الغردقة، جمهورية مصر العربية، 2005م، ص 3 /25/8.

2 وائل أنور بندق بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، لعام 2007م، ص 35 وما بعدها.

3 UNCITRAL Model Law on Electronic Signatures, (2001) 32 Y.B. U.N. CommissionInt’l Trade L. 499, U.N Doc. A/CN.9/SER.A/2001.

ولم يقيّد هذا القانون مفهوم التوقيع الإلكتروني، بل إنّ هذا النص السابق يمكن أن يستوعب أيّة تقنية تظهر في المستقبل تعنى بإنشاء التوقيع الإلكتروني. ولا يستبعد هذا القانون أيّة تقنيات حديثة تظهر مستقبلاً خاصّة بإنشاء التوقيع الإلكتروني ما دامت تتوافق مع المتطلبات التي اشترطها[1].

وقد أصدر المشرع الفرنسي قانون التوقيع الإلكتروني رقم (230) لعام 2000م، في شكل تعديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي بما يجعلها متماشية مع تقنية المعلومات، وازدياد استخدام التوقيع الإلكتروني في التعاملات الإلكترونية، وقد تم إدراج هذا التعديل ضمن نصّ المادة (1316) من قانون التوقيع الإلكتروني الفرنسي، وقد ورد ضمن أحكام هذا القانون أن التوقيع الإلكتروني يدلّ على شخصية الموقِّع وتضمن علاقته بالواقعة المنسوبة إليه، كما يؤكّد صحّة الواقعة المنسوبة إليها هذا التوقيع إلى أن يثبت العكس.

وقد أضفى المشرع الفرنسي على الكتابة الإلكترونية والمحررات الإلكترونية والتوقيع الإلكتروني الحجية في الإثبات شأنها في ذلك شأن المحررات والكتابة الخطية والتوقيع الخطي التقليدي[2]، إذ نصّت المادة (1316/ 1) من قانون التوقيع الإلكتروني الفرنسي على أنه ((تتمتّع الكتابة الإلكترونية بذات الحجية المعترف بها للمحررات الكتابية في الإثبات، شريطة أن يكون بالإمكان تحديد شخص مصدرها

1 Draft Guide to Enactment of UNCITRAL Model law on Electronic Signatures :Note by the Sceretatiat, U.N .GAOR, 34th Sess. , at 17-18 , cmt. 32. U.N. Doc.A/CN.9/493 (2001) , reprinted in) 2001) 32 Y.B. U.N. Commission Int'l Trade L.313, 321-22 , Cmt. 32, U.N. Doc. A.CN. 9/SER. A/ 2001.

2 منري محمد الجنبيهي وممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، مرجع سابق، ص 89 وما بعدها . انظر أيضًا: ممدوح محمد مبروك، مرجع سابق، ص128.

على وجه الدقة، وأن يكون تدوينها وحفظها قد تم في ظروف تدعو إلى الثقة))، ونصّت المادة (3/1316) من القانون ذاته على أنه ((يكون للكتابة على دعامة إلكترونية ذات الحجية في الإثبات التي للمحررات الورقية)). وبذلك يكون المشرع الفرنسي قد قبل الكتابة الإلكترونية مثل الكتابة التقليدية، كما قبل هذه الكتابة دليلاً في الإثبات مثل الكتابة الورقية شريطة أن تعبّر عن شخصية واضعيها[1]. ومن ثمّ فإنّ المشرع الفرنسي قد خطا خطوة مهمّة في مجال تطوير التجارة الإلكترونية، خاصة فيما يتعلق بالمساواة بين المحررات الكتابية التقليدية والمحررات الإلكترونية، وكذلك المساواة بين التوقيع التقليدي الكتابي والتوقيع الإلكتروني. كما يلاحظ أنّ قانون التوقيع الإلكتروني الفرنسي قد صدر استجابة للتوجيه الأوروبي رقم (93) لعام 1999م، والمتضمن جعل القوانين الوطنية الأوروبية منسجمة مع أحكام ونصوص التوجيه الأوروبي في هذا الخصوص. واستجابة كذلك لتوجيهات الأمم المتحدة التي دعت دول العالم كافة إلى ضرورة إصدار تشريعات وطنية لتنظيم التجارة الإلكترونية الدولية، وتعترف بحجية التوقيع الإلكتروني)[2].

---

1 فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، مرجع سابق، ص256 . انظر أيضًا : عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني، مرجع سابق . انظر أيضًا: عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني، مرجع سابق . ص474 وما بعدها.

2 وأن تكون على نهج قانون الأونسيترال (UNCITRAL) النموذجي لعام 1996 المتعلق بالتجارة الإلكترونية، والذي أعدّته لجنة الأمم المتحدة لقانون التجارة الدولي، والذي تبنّته منظمة التجارة العالمية (WTO) ضمن الإطار العام الذي وضعته بشأن تسهيل التعاملات التجارية . انظر: عبد الفتاح بيومي حجازي، مرجع سابق . ص 475 وما بعدها . انظر أيضًا: ثروت عبد الحميد، مرجع سابق. ص173 وما بعدها، انظر أيضًا: ممدوح مبروك، مرجع سابق. ص 129 وما بعدها.

وقد أقرّ القانون الإنجليزي بالحجية للتوقيع الإلكتروني تمامًا كالتوقيع التقليدي وبموجب قانون الاتصالات الإلكتروني لعام 2000م. والذي دخل حيّز التنفيذ في 30 يوليو 2000م. ويشكّل هذا القانون إضافة إلى لوائح التوقيعات الإلكترونية لعام 2002م الأساس القانوني للتوقيعات الإلكترونية في المملكة المتحدة المتحدة.

وقد تبنّت المملكة المتحدة وطبّقت أحكام نصوص التوجيه الخاص بالاتحاد الأوروبي بشأن التجارة الإلكترونية ضمن نصوص قانون الاتصالات الإلكترونية لعام 2000م[1]، ويعرّف قانون الاتصالات الإنجليزي التوقيع الإلكتروني بأنه ((بيانات إلكترونية)) ترتبط بشكل منطقي بالبيانات الإلكترونية الأخرى، وهذا يخدم في مسألة التصديق. كما تضمّنت لوائح التوقيعات الإلكترونية لعام 2002م مفهوم التوقيع الإلكتروني المتقدم، والذي يعتبر توقيعًا أكثر أمانًا، بمعنى أنه يعتبر وكأنه توقيع تقليدي خطي ويحتوي التوقيع الإلكتروني على خصائص مثل أن يحدّد هوية الموقِّع، ويرتبط بشكل صريح بالموقِع، وتحت سيطرة وتحكم الموقِّع دون غيره، ويرتبط بالبيانات بطريقة تجعل أيّ تغيير لاحق يمكن ملاحظته بسهولة.

وينصّ قانون الاتصالات الإلكترونية لعام 2000م على قبول التوقيعات الإلكترونية كدليل أمام المحاكم شريطة توافر أن يكون التوقيع مصدقًا، وأن يكون جزءًا من رسالة إلكترونية.

ويعترف القانون الإنجليزي بالتوقيعات الإلكترونية الصادرة من دول الاتحاد الأوروبي الأخرى ما دامت متوافقة مع الشروط التي حدّدها القانون الإنجليزي للتوقيعات الإلكترونية.

---

1 European Union Electronic Commerce Directive, 1999/93/EC.

وبما أنّ التوقيع الإلكتروني في المملكة المتحدة هو أيّ بيانات إلكترونية مرتبطة أو متعلّقة ببيانات إلكترونية أخرى، فمن الممكن الاستنتاج من هذا التعريف أنّ مسمى التوقيعات الإلكترونية ينطبق ليس فقط على مراسلات البريد الإلكتروني[1] .

وقد حكمت إحدى المحاكم البريطانية في قضية (بي أن سي) في عام 2002م بأنّ الخطاب المرسل كان بواسطة جهاز الفاكسيملي. والتوقيع الملحق بهذا الإرسال يعدّ صحيحًا كإبلاغ لحملة الحصص بموجب قانون الشركات لعام 1983م وقانون الاتصالات الإلكترونية لعام 2000م السالف الذكر[2]، ولكن لا تزال مشكلة تأمين التوقيعات الإلكترونية تثير قلق المؤسسات التجارية، وتحدّ من استخدام التوقيع الإلكتروني في بريطانيا. وقد طبّقت دول الاتحاد الأوروبي الخمس والعشرين جميعها التوجيه الأوروبي السالف الذكر بشأن التجارة الإلكترونية والتوقيع الإلكتروني. ويذكر الخبراء في التقنية أن تزوير التوقيع الإلكتروني أصعب من تزوير التوقيع التقليدي المكتوب بخط اليد. وقد كان من المقرّر أن توقّع ملكة بريطانيا على مشروع قانون الاتصالات الإلكترونية باستخدام التوقيع الإلكتروني، إلا أن هذا الأمر تم التخلي عنه بعدما تبيّن أن التوقيع الإلكتروني لجلالتها لم يكن يعد توقيعًا قانونيًّا إلا بعد أن توقعه خطيًّا بالشكل التقليدي[3].

ومع التطور الذي حدث للتجارة الإلكترونية في الولايات المتحدة الأمريكية في التسعينيات من القرن الماضي، بدأت العديد من الولايات في إصدار تشريعات تنظم

---

1 BBC News, Business, Digital Signature becomes Law, at : http://news.bbc.co.uk/2/ hi/business/1446426
2 PNC Telecom V. Thomas (2002) EWHC 284 (Ch)
3 BBC news, Clinton Oks, e-signatures at http://news.bbc.co.uk/2hi/science/nature/813437.stn

الاعتراف بالتوقيع الإلكتروني في الإثبات[1] لكن الحكومة الفيدرالية الأمريكية رغبت في توحيد القوانين ذات العلاقة بالتوقيع الإلكتروني على المستوى الفيدرالي. بما يسهم في إزالة الاختلافات بين تشريعات الولايات المختلفة، وبما يحقّق التوافق فيما بينها، ومن ثم تدعيم الثقة في التعاملات الإلكترونية.

وتمّ إصدار القانون الموحّد للتعاملات الإلكترونية، وهو قانون نموذجي تم الأخذ به واعتماده في غالبية الولايات الأمريكية. ويهدف هذا القانون إلى تسهيل التجارة الإلكترونية عبر إعطاء الاتفاقيات الإلكترونية والتوقيعات الإلكترونية ذات الحجية التي تتمتّع بها الاتفاقيات والتوقيعات اليدوية[2]، وينصّ القسم السابع من هذا القانون على أنّ للتوقيع الإلكتروني ذات الحجية في الإثبات التي يتمتّع بها التوقيع اليدوي. وأنه إذا تطلب القانون وجود توقيع، فإنّ التوقيع الإلكتروني يحقّق متطلّبات هذا القانون[3]، ويعرّف هذا القانون التوقيع الإلكتروني بأنه أيّ صوت أو رمز أو إجراء إلكتروني مرتبط أو متعلّق منطقيًّا بسجل وينفذ أو يعتمد من الشخص الراغب في توقيع السجل.

---

1 Ian A. Rambarran, I Accept But Do They? : The Need for Electronic Signature Legislation on Mainland China, 15 TRANSNAT'L Law 405, 417-18, (2002).

2 UNIF. ELEC. TRANSACTIONS Act, 7A U.L.A.23 (2002 and supp.. 2004) See also Christopher William Pappas, Comparative U.S and EU Approaches to Ecommerce Regulations : Jurisdiction, Electronic Contracts, Electconic Signatures and Taxation, 31 DENV. J. INT.LL and Poly 325, 341 (2002).

3 UNIF. ELEC. TRANACTIONS Act, 7A U.L.A.252, 2002.

كما أصدرت الولايات المتحدة الأمريكية قانون التوقيع الإلكتروني في التجارة[1]، ووقع على هذا القانون الرئيس الأمريكي بيل كلينتون في 30 يونيو عام 2000م بعد أن أقرّه الكونجرس بمجلسيه، ودخل هذا القانون حيّز التنفيذ في أكتوبر من عام 2000م[2].

وكان سبب إصدار هذا القانون هو الوصول إلى توحيد قوانين التجارة الإلكترونية في الولايات المختلفة، ويحقّق نوعًا من الانسجام والتوافق فيما بينها، ومن ثم يدعم الثقة في التعاملات الإلكترونية.

وهذا القانون ذو طبيعة إجرائية ولا يحلّ محلّ قوانين العقود وما تتضمّنه تلك القوانين من أحكام[3]، ويطبق هذا القانون على التصرفات والتعاملات الإلكترونية التي ينتمي أطرافها إلى ولايات مختلفة، وعلى التصرفات القانونية التي تتم مع أطراف أجنبية خارج الولايات المتحدة، ويعترف هذا النظام بحجية المحررات الإلكترونية والتوقيعات الإلكترونية في الإثبات، ولا يتطلّب هذا القانون الحصول على شهادة توثيق تثبت موافقة أو قبول جهة أخرى على هذا التوقيع[4].

---

1 Electronic Signatures in Global and National Commerce Act. 15 U. S.C. *ff* 7001- 7031 (2000).

2 Amy J. Dunn, Survey of Legislation: Uniform Electronic Transactions, 24 U, (2000): ARK. LITTLE ROCK. L.REV. 603 , 612 (2002). See also Benjamin Suksomnil, An Analysis of the Electronic Signatures in Global and National Commerce Act and Its Effects on E-commerce and the Online Consumer, 2002, SYRACUSE L and TECH. J. 2t, and V.

3 فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، مرجع سابق، ص 256. انظر أيضًا: ثروت عبد الحميد، التوقيع الإلكتروني، مرجع سابق، ص 186 وما بعدها.

4 فيصل الغريب، مرجع سابق، ص 256. انظر أيضًا: ثروت عبد الحميد، مرجع سابق، ص 187.

ولا تطبّق أحكام هذا القانون على العقود والمحررات الخاضعة لنصوص التشريعات الخاصة بالوصايا والميراث، والتشريعات الخاصة بالمسائل العائلية، ونصوص القانون التجاري الموحّد وأوراق المحاكم، والمحرّرات الخاصة بإثبات اتفاقيات الائتمان[1].

ونخلص ممّا سبق إلى أنه بما أن التوقيع الإلكتروني أثبت قدرته على أداء مهام التوقيع الكتابي التقليدي، فلا بد من دعوة المشرع الإماراتي لاعتماد هذا التوقيع الإلكتروني، ومنحه القوة الثبوتية أمام المحاكم، والجهات الحكومية، ولا بد من منح المستندات الإلكترونية القوة الممنوحة للمستندات الورقية التقليدية، إذ أصبح هذا واقعًا لا مفرّ منه في ظلّ التطورات الحالية في المعاملات التجارية الدولية عبر شبكة الإنترنت، وهذا ما جعل الاعتراف بالتوقيع الإلكتروني والمستندات الإلكترونية مسألة ضرورية بما يمكن الأطراف المتعاقدة من تقديم المستندات بعد استخراجها من الحاسب الآلي وتوقيعها إلكترونيًا، وعدّها أدلة للإثبات تقدم إلى الجهات القضائية[2].

المطلب الثاني: دور التوقيع الإلكتروني في الإثبات

يعدّ التوقيع حجر الزاوية في نظام الإثبات باعتباره شرطًا جوهريًا في الدليل الكتابي، أمّا الكتابة في حدّ ذاتها، فبالرغم من أنها شرط بديهي لوجود المحرر، فإنها لا ترقى من الناحية القانونية إلى مرتبة الدليل الكامل في الإثبات، إلا إذا كانت تحمل توقيع من يحتج بها عليه، لذلك من المستقر عليه فقهًا وقضاء أنّ التوقيع هو الشرط الوحيد لصحة المحرّر العرفي للإثبات، والمصدر الوحيد لحجية ما ورد فيه.

---

1 ثروت عبد الحميد، مرجع سابق، ص 187 وما بعدها.

2 يحيى يوسف فلاح حسن، مرجع سابق، ص 95.

لقد تأثّرت فكرة التوقيع بفعل التطور المستمر في نظم المعالجة الآلية للمعلومات، والتقدم التقني في وسائل الاتصال، وقد ساعد ذلك على ظهور أنماط عديدة من التوقيعات الإلكترونية في الواقع العملي، الأمر الذي أثار العديد من التساؤلات حول مدى إمكانية الاعتداد بها في مجال الإثبات.

ولقد نصّ قانون المعاملات والتجارة الإلكترونية لإمارة دبي[1] على أنه "يعامل التوقيع على أنه توقيع إلكتروني محميّ إذا كان من الممكن التحقّق من خلال تطبيق إجراءات توثيق محُكمة منصوص عليها في هذا القانون أو معقولة تجاريًّا ومتفق عليها بين الطرفين، ويشترط فيه أن التوقيع الإلكتروني كان في الوقت الذي تم فيه، وينفرد به الشخص الذي استخدمه، ومن الممكن أن يثبت هوية ذلك الشخص، وأن يكون تحت سيطرته التامة سواء بالنسبة لإنشائه أم وسيلة استعماله وقت التوقيع، ويرتبط بالرسالة الإلكترونية ذات الصلة به أو بطريقة توفر تأكيدًا يعول عليه حول سالمة التوقيع، بحيث إذا تم تغيير السجل الإلكتروني فإنّ التوقيع يصبح غير محمي"[2].

وكذلك نصّ القانون على عقوبة كلّ من أنشأ أو نشر أو وفر أية شهادات أو بيانات غير صحيحة لأيّ غرض احتيالي، أو أيّ غرض آخر غير مشروع، بالحبس أو بغرامة لا تجاوز 250.000 درهم أو بإحدى هاتين العقوبتين[3]. و"مع عدم الإخلال بأية عقوبات أشدّ ينص عليها قانون آخر، يعاقب كل من قدم متعمدًا بيانات

---

1 المادة (20) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي.

2 قانون رقم (2002) بشأن المعاملات والتجارة الإلكترونية الخاص بإمارة دبي.

3 المادة (29) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي.

غير صحيحة عن هويته أو تفويضه إلى مزود خدمات التصديق بغرض طلب استصدار أو إلغاء أو إيقاف شهادة، بالحبس مدة لا تزيد على ستة أشهر، وبغرامة لا تتجاوز 100.000 درهم أو بإحدى هاتين العقوبتين"[1]. وقد أعطى هذا القانون في الفقرة (3) من المادة (12) منه كامل الحجية للتوقيع الإلكتروني التي يتمتّع بها التوقيع التقليدي[2].

كما أصدر المشرع الإماراتي القانون الاتحادي للمعاملات والتجارة الإلكترونية لعام 2006م، والذي عرف التوقيع الإلكتروني بأنه ((توقيع مكوّن من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط منطقيًّا برسالة إلكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة[3]. ونصّ هذا القانون على سريانه على السجلات والمستندات والتوقيعات الإلكترونية ذات العلاقة بالمعاملات والتجارة الإلكترونية، ويهدف هذا القانون إلى تسهيل وإزالة أيّة عوائق أمام التجارة الإلكترونية والمعاملات الإلكترونية الأخرى، والتي قد تنتج عن

1 المادة (30) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي.

2 ومن مظاهر الحجية التي أسبغها هذا القانون على التوقيع الإلكتروني: إمكانية التعديل عليه في جميع المعاملات والتصرفات القانونية. ويفترض هذا القانون أنّ صاحب التوقيع الإلكتروني وضع توقيعه بنية توقيع الرسالة؛ أي: أنّ نيته وإرادته اتجهت نحو سريان موضوع الرسالة أو التصرف القانوني في حقّه، وبالتالي تحمّل كافة الالتزامات والحقوق الناتجة عن ذلك. انظر: محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، مرجع سابق، ص245 وما بعدها. انظر أيضًا: فيصل الغريب، التوقيع الإلكرتوني وحجيته في الإثبات، مرجع سابق، ص 255 وما بعدها.

3 المادة (1)، القانون الاتحادي الإماراتي رقم (1) لعام2006م في شأن المعاملات والتجارة الإلكترونية.

الغموض المتعلّق بمتطلبات الكتابة والتوقيع وتعزيز التطور القانوني والتجاري لتطبيق التجارة الإلكترونية بصورة مضمونة[1].

كذلك نصّ هذا القانون على أنه إذا اشترط القانون وجود توقيع على مستند أو نصّ على ترتيب نتائج معينة على التوقيع، فإنّ التوقيع الإلكتروني يستوفي ذلك الشرط[2].

ومن ثمّ فإنّ المشرع الإماراتي يكون قد أعطى ذات الحجية للتوقيع الإلكتروني التي أعطاها للتوقيع التقليدي. وبذلك يكون المشرع الإماراتي قد خطا خطوات مهمّة نحو التجارة الإلكترونية وتدعيمها[3].

ولا يوجد ما يمنع أو يقيّد حرية الأطراف في الاتفاق على الأخذ بأيّ شكل من أشكال التوقيع الإلكتروني في إثبات تصرّفاتهم التعاقدية. باستثناء بعض التصرفات التي يتطلب القانون لها شكلاً، بحيث لا يتم سريانها إلا باستيفائها هذا الشكل، مثل العقود التي تحتاج إلى تصديق الكاتب العدل، أو توقيعها أمام موظّف عام بصورة

---

1 فقرة (3)، مادة (3) القانون الاتحادي الإماراتي رقم (1) لعام 2006م في شأن المعاملات والتجارة الإلكترونية.

2 فقرة (1) مادة (8)، القانون الاتحادي الإماراتي رقم (1) لعام 2006م في شأن المعاملات والتجارة الإلكترونية.

3 فإضافة إلى إنشاء مدينة دبي للإنترنت، وهي منطقة حرة للتقنية أنشأتها حكومة دبي مرجعًا لجميع شركات تقنية المعلومات. تسعى كلّ من حكومتي دبي وأبوظبي وباقي الإمارات الأخرى إلى تدعيم الوصول إلى تطبيق شامل للحكومة الإلكترونية. انظر: محمد عبيد الكعبي، مرجع سابق، ص 245. انظر أيضًا: فيصل الغريب، مرجع سابق، ص 255.

رسمية، وبخلاف ذلك لا حرج في الأخذ بالتوقيعات الإلكترونية كوسيلة من وسائل الإثبات[1].

ولهذا وبما أنّ قضايا التشريع والقانون تختلف دائمًا عن التغيرات التي تطرأ على التكنولوجيا، فلا يكون أمامنا إلا الأخذ بهذه المفاهيم المتطورة في الإثبات، وهذا ليس من أجل التطور فحسب، إنما لأنّ هذا التطور مفروض علينا وليس أمامنا خيار إلا الأخذ به.

وقد أخذ المشرع الإماراتي في الاعتبار لحجية المحرر الإلكتروني الطرق المستخدمة في الحفظ وسلامة المعلومات والاعتداد بمصدر المعلومات، وبطريقة التأكد من هوية المنشئ وبأيّ عناصر أخرى متصلة بالموضوع، وإذا كانت المحررات الإلكترونية تظهر أهميتها في قابليتها للاحتفاظ بالمعلومات والرجوع إليها متى أراد الأطراف المتعاقدة ذلك، وتخزينها لتكون حجة في الإثبات وتعطي الثقة والأمان لمثل هذه المعاملات الإلكترونية، وهذا هو غاية المحررات والمستندات الورقية والكتابية، فلا عجب أن تعطي القوانين السابقة نفس القوة للمحرر الإلكتروني كالمحرر الورقي الكتابي .

وإدراكًا من المشرع الإماراتي بأنّ غياب التنظيم القانوني للتوقيع الإلكتروني يؤدّي إلى إثارة العديد من المشاكل القانونية لعدم إمكانية قبوله من القضاء، الأمر الذي يؤدّي إلى حرمان الأفراد من امتلاك الأدلة على إثبات تصرفاتهم التعاقدية، فقد صدر وفقًا للقانون الاتحادي الإماراتي بشأن المعاملات والتجارة الإلكترونية والذي

---

1 عبد الحميد، رائد، مجلة العدالة والقانون، مدى حجية وسائل الإتصال الحديثة في قانون البينات، العدد (2)، تموز سنة 2005م، رام الله، ص30.

نصّ صراحة على حجية التوقيع الإلكتروني[1]، "إذا اشترط القانون وجود توقيع على مستند أو نص على ترتيب نتائج معيّنة على التوقيع، فإنّ التوقيع الإلكتروني الذي يعتمد عليه في إطار المعنى الوارد في المادة (18) من هذا القانون يستوفي ذلك الشرط، ويجوز لأيّ شخص أن يستخدم أيّ شكل من أشكال التوثيق الإلكتروني، إلا إذا نص القانون على غير ذلك".

وإذا اشترط القانون تقديم الرسالة الإلكترونية أو الاحتفاظ بها في شكلها الأصلي أو رتّب على عدم توفر ذلك نتائج معينة، فإنّ الرسالة الإلكترونية تعتبر أصلية إذا تحقق الآتي[2]: إذا وجد ما يعتد به فنيًّا لتأكيد سلامة المعلومات الواردة في الرسالة الإلكترونية منذ الوقت الذي أنشئت فيه للمرة الأولى في شكلها النهائي كمستند أو سجل إلكتروني، ويكون معيار تقدير سلامة المعلومات هو تحديد ما إذا كانت قد بقيت مكتملة ودون تغيير، باستثناء أيّة إضافة أو تظهير أو تغيير يطرأ أثناء الوضع العادي للإبلاغ والتخزين والعرض، وتقدر درجة الاعتداد المطلوب على ضوء الغرض الذي أنشئت من أجله المعلومات، وعلى ضوء الظروف ذات الصلة، وإذا كانت الرسالة تسمح بعرض المعلومات المطلوب تقديمها متى طلب ذلك.

---

1 المادة (8) من القانون الاتحادي الإماراتي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية.

2 المادة (9) من القانون الاتحادي الإماراتي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية.

وقدإشترط القانون الاتحادي الإماراتي بشأن المعاملات والتجارة الإلكترونية في قبول وحجية البينة الإلكترونية، فنصّ على[1] أن لا يحول دون قبول الرسالة الإلكترونية أو التوقيع الإلكتروني كدليل إثبات أن تكون الرسالة أو التوقيع قد جاء في شكل إلكتروني، وأن تكون الرسالة أو التوقيع ليس أصليًّا أو في شكله الأصلي، متى كانت هذه الرسالة أو التوقيع الإلكتروني أفضل دليل يتوقّع بدرجة معقولة أن يحصل عليه الشخص الذي يستشهد به.

وفي تقدير حجية المعلومات الإلكترونية في الإثبات، تراعى مدى إمكانية الاعتداد بالطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات إدخال المعلومات أو إنشائها أو تجهيزها أو تخزينها أو تقديمها أو إرسالها، ومدى إمكانية الاعتداد بالطريقة التي استخدمت في المحافظة على سلامة المعلومات، ومدى إمكانية الاعتداد بمصدر المعلومات إذا كان معروفًا، ومدى إمكانية الاعتداد بالطريقة التي تم بها التأكّد من هوية المنشئ، وأيّ عنصر آخر يتصل بالموضوع ما لم يتم إثبات عكس ذلك، يفترض أن التوقيع الإلكتروني المحمي يمكن الاعتداد به، وهو توقيع الشخص الذي تكون له صلة به، وقد وضعه ذلك الشخص بنية توقيع أو اعتماد الرسالة الإلكترونية المنسوب إليه إصدارها، وما لم يتم إثبات عكس ذلك يفترض أن السجل الإلكتروني المحمي لم يتغير منذ أن أنشئ ومعتد به.

ولقد نصّت المادة (17) مكرر من القانون رقم (36 /2006) بتعديل أحكام قانون الإثبات في المعاملات المدنية والتجارية الصادر بالقانون الاتحادي رقم

---

1 المادة (10) من القانون الاتحادي الإماراتي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية.

(1992/10) على أن "يعتبر توقيعًا إلكترونيًّا كلّ أحرف أو أرقام أو رموز أو إشارات أو صور أو أصوات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره على النحو الوارد في قانون المعاملات والتجارة الإلكترونية، ويعتبر محررًا إلكترونيًّا كل انتقال أو إرسال أو استقبال أو تخزين لرموز أو إشارات أو كتابة أو صور أو أصوات أو معلومات أيًّا كانت طبيعتها تجري من خلال وسيلة تقنية معلومات، وللتوقيع الإلكتروني ذات الحجية المقررة للتوقيعات المشار إليها في هذا القانون إذا روعي فيه الأحكام المقررة في قانون المعاملات والتجارة الإلكترونية، وللكتابة الإلكترونية والمحررات الإلكترونية والسجلات والمستندات الإلكترونية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام هذا القانون متى استوفت الشروط والأحكام المقررة في قانون المعاملات والتجارة الإلكترونية[1].

فالمادة (17) مكرّر أعطت للمحررات الإلكترونية والكتابة الإلكترونية والتوقيع الإلكتروني نفس الحجية المقررة للتوقيعات والمحررات المذكورة في قانون الإثبات في المعاملات المدنية والتجارية متى استوفت الشروط والأحكام المقررة في قانون المعاملات والتجارة الإلكترونية.

كما نصّ قانون المعاملات والتجارة الإلكترونية لإمارة دبي[2] على أن "يكون للمعلومات الإلكترونية ما تستحقّه من حجية في الإثبات، وفي تقدير هذه الحجية

---

1 المادة (17) مكرر من القانون رقم (36/ 2006) بتعديل أحكام قانون الإثبات فى المعاملات المدنية والتجارية الصادر بالقانون الاتحادي رقم 1992/10.

2 المادة (12) من قانون المعاملات والتجارة الإلكترونية رقم (2002/2) لإمارة دبي.

يعطي الاعتبار لمدى إمكانية التعويل على الطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات الإدخال أو الإنشاء أو التجهيز أو التخزين أو التقديم أو الإرسال، ومدى إمكانية التعويل على الطريقة التي استخدمت في المحافظة على سلامة المعلومات، ومدى إمكانية التعويل على مصدر المعلومات إذا كان معروفًا، ومدى إمكانية التعويل على الطريقة التي تم بها التأكد من هوية المنشئ، إذا كان ذلك ذا صلة، وأيّ عامل آخر يتصل بالموضوع، أمّا في غياب البينة المناقضة، يفترض أن التوقيع الإلكتروني المحمي يمكن التعويل عليه، وهو توقيع الشخص الذي تكون له صلة به، وقد وضعه ذلك الشخص بنية توقيع أو اعتماد الرسالة الإلكترونية التي ألحقت أو اقترنت به بصورة منطقية.

الأمر الذى يكون أعطى القانون الإماراتي الاتحادي أو المحلي للتوقيع الإلكتروني أو المحرر الإلكتروني كافة الحجية المقررة للمحررات العادية في الإثبات[1].

ولقد تناول نظام التعاملات الإلكترونية السعودي حجية التوقيع الإلكتروني في الإثبات في القانون السعودي الصادر عام 1428 هـ، ونصّ على[2] أن "يكون للتعاملات والسجلات والتوقيعات الإلكترونية حجيتها الملزمة، ولا يجوز نفي صحتها أو قابليتها للتنفيذ ولا منع تنفيذها بسبب أنها تمت -كلّيًا أو جزئيًا- بشكل إلكتروني

---

1 مجدى أحمد عزام، الحجية القانونية للتوقيع الإلكتروني والمعاملات الإلكترونية في القوانين العربية "دراسة مقارنة"، منتدى المحامين العرب، منشور على الموقع الإلكتروني، تاريخ الاطلاع عليه: 20 - 2-2017م.
http://www.mohamoon.com/MONTADA/Default.aspx?Action=Display&ID=117932&Type=3 ،

2 المادة (5) من نظام التعاملات الإلكترونية السعودي.

بشرط أن تتم تلك التعاملات والسجلات والتوقيعات الإلكترونية بحسب الشروط المنصوص عليها في هذا النظام، ولا تفقد المعلومات التي تنتج من التعامل الإلكتروني حجيتها أو قابليتها للتنفيذ متى كان الاطلاع على تفاصيلها متاحًا ضمن منظومة البيانات الإلكترونية الخاصة منشؤها وأشير إلى كيفية الاطلاع عليها".

" ويقبل التعامل الإلكتروني أو التوقيع الإلكتروني دليلاً في الإثبات إذا استوفى سجلّه الإلكتروني متطلبات حكم المادة (الثامنة) من هذا النظام، ويجوز قبول التعامل الإلكتروني أو التوقيع الإلكتروني قرينة في الإثبات، حتى إن لم يستوف سجلّه الإلكتروني بمتطلبات حكم المادة (الثامنة) من هذا النظام، ويعدّ كلّ من التعامل الإلكتروني والتوقيع الإلكتروني والسجل الإلكتروني حجّة يعتدّ بها في التعاملات، وأن كلاً من على أصله (لم يتغير منذ إنشائه) ما لم يظهر خلاف ذلك، ويراعى عند تقدير حجية التعامل الإلكتروني مدى الثقة في الطريقة التي استخدمت في إنشاء السجل الإلكتروني أو تخزينه أو إبلاغه، وإمكان التعديل عليه، والطريقة التي استخدمت في المحافظة على سلامة المعلومات، والطريقة التي حددت بها شخصية المنشأ."[1] و"مع عدم الإخلال بما تنصّ عليه المادة (الثالثة) من هذا النظام، إذا اشترط أيّ نظام في المملكة أن تكون الوثيقة أو السجل أو المعلومة المقدّمة إلى شخص آخر مكتوبة، فإنّ تقديمها في شكل إلكتروني يفي بهذا الغرض متى تحقّقت الأحكام الواردة في الفقرة (1) من المادة (السادسة)"[2]، و"إذا اشترط وجود توقيع خطّيّ على مستند أو عقد أو نحوه، فإنّ التوقيع الإلكتروني الذي يتم وفقًا لهذا النظام

---

1 المادة (5) من نظام التعاملات الإلكترونية السعودي.

2 المادة (7) من نظام التعاملات الإلكترونية السعودي.

يعدّ مستوفيًا لهذا الشرط، ويعدّ التوقيع الإلكتروني بمثابة التوقيع الخطي، وله الآثار النظامية نفسها[1].

يجب على من يرغب في إجراء توقيع إلكتروني أن يقوم بذلك وفقًا لأحكام هذا النظام والضوابط والشروط والمواصفات التي تحدّدها اللائحة، وعليه مراعاة واتخاذ الاحتياطات اللازمة لتلافي أيّ استعمال غير مشروع لبيانات إنشاء التوقيع، أو المعدات الشخصية المتعلّقة بتوقيعه. وتحدّد اللائحة تلك الاحتياطات، وإبلاغ مقدم خدمات التصديق عن أيّ استعمال غير مشروع لتوقيعه وفق الإجراءات التي تحددها اللائحة، أمّا إذا قدم توقيع إلكتروني في أيّ إجراء شرعي أو نظامي، فإنّ الأصل – ما لم يثبت العكس أو تتفق الأطراف المعنية على خلاف ذلك– صحة الأمور الآتية: أن التوقيع الإلكتروني هو توقيع الشخص المحدد في شهادة التصديق الرقمي، وأن التوقيع الإلكتروني قد وضعه الشخص المحدد في شهادة التصديق الرقمي، وبحسب الغرض المحدد فيها، وأن التعامل الإلكتروني لم يطرأ عليه تغيير منذ وضع التوقيع الإلكتروني عليه، وإذا لم يستوف التوقيع الإلكتروني الضوابط والشروط المحددة في هذا النظام واللائحة، فإنّ أصل الصحة المقرر بموجب الفقرة (3) من هذه المادة لا يقوم للتوقيع ولا للتعامل الإلكتروني المرتبط به، ويجب على من يعتمد على التوقيع الإلكتروني لشخص آخر أن يبذل العناية اللازمة للتحقّق من صحة التوقيع، وذلك باستخدام بيانات التحقق من التوقيع الإلكتروني، وفق الإجراءات التي تحددها اللائحة.

---

1 المادة (14) من نظام التعاملات الإلكترونية السعودي.

فالقانون السعودي أعطى للتوقيع الإلكتروني نفس الحجية التي هي للتوقيع الخطي، وأعطى له نفس الآثار القانونية المقررة للتوقيع الخطي متى تم التوقيع الإلكتروني وفقًا للقواعد واللوائح المنصوص عليها في القانون، كما اعترف القانون بالمعاملات الإلكترونية والتوقيع الإلكتروني كدليل في الإثبات متى استوفت شروطها، ويعتبر حجة على الكافة ولا يجوز نفي حجيتها وقوتها الملزمة[1].

إنّ المشرع المصري قد نصّ هو الآخر على حجية التوقيع الإلكتروني في الإثبات بقوله: "للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للتوقيعات في أحكام المحرر، إثبات في المواد المدنية والتجارية، إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحدّدها اللائحة التنفيذية لهذا القانون، وللكتابة الإلكترونية وللمحررات الإلكترونية، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى استوفت الشروط المنصوص عليها في هذا القانون وفقًا للضوابط الفنية والتقنية التي تحدّدها اللائحة التنفيذية لهذا القانون، وللصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي حجة على الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر، وذلك ما دام المحرر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين على الدعامة الإلكترونية، وتسري في شأن إثبات صحة المحررات الإلكترونية الرسمية والعرفية والتوقيع الإلكتروني،

---

1 مجدي أحمد عزام، الحجية القانونية للتوقيع الإلكتروني والمعاملات الإلكترونية في القوانين العربية "دراسة مقارنة"، مرجع سابق.

فيما لم يرد بشأنه نصّ في هذا القانون أو في لائحته التنفيذية الأحكام المنصوص عليها في قانون المرافعات المدنية والتجارية[1].

ويتمتّع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها شروط مثل[2] ارتباط التوقيع بالموقّع وحده دون غيره، وسيطرة الموقّع وحده دون غير على الوسيط الإلكتروني، وإمكانية كشف أيّ تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني، وتحدّد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك.

وعليه فإنّ للتوقيع الإلكتروني والمحرر الإلكتروني في القانون المصري بل والصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي ذات الحجية القانونية المقررة للتوقيعات والمحررات الرسمية والعرفية في أحكام الإثبات المصري متى استوفت الشروط القانونية[3].

وإذا لم يرد بشأنه نصّ في حجية وإثبات التوقيع الإلكتروني والمحرر الإلكتروني الرجوع إلى القواعد المذكورة في قانون الإثبات المصري.

أمّا عن شروط تمتّع التوقيع الإلكتروني والمحرر الإلكتروني في الإثبات وفقًا لقانون التوقيع الإلكتروني فهي[4] ثبوت أن التوقيع الإلكتروني مرتبط ارتباط شخص بالموقع "صاحب التوقيع"، وأن يكون لصاحب التوقيع وحده دون غيره السيطرة على

---

1 المواد (14 إلى 17) من قانون التوقيع الإلكتروني رقم 2004/15.

2 المادة (18) من قانون التوقيع الإلكتروني رقم 2004/15.

3 مجدي أحمد عزام، الحجية القانونية للتوقيع الإلكتروني والمعاملات الإلكترونية في القوانين العربية "دراسة مقارنة"، مرجع سابق.

4 نفس مرجع سابق.

الوسيط الإلكتروني، وأن يكون من الممكن معرفه وكشف أيّ تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني، فمتى توافرت تلك الشروط كان للتوقيع الإلكتروني حجية الإثبات.

ونصّ قانون الإثبات في المواد المدنية والتجارية المصري[1] على "أن المحررات الرسمية حجة على الناس كافة بما دوّن فيها من أمور قام بها محررها في حدود مهمته أو وقعت من ذوي الشأن في حضوره ما لم يثبت تزويرها بالطرق المقررة قانونًا"، و"يعتبر المحرر العرفي صادرًا ممّن وقعة ما لم ينكر صراحة ما هو منسوب إليه من خط أو إمضاء أو ختم أو بصمة"، أمّا الورثة أو الخلف فلا يطلب منه الإنكار، ويكفي أن يحلف يمينًا بأنه لا يعلم أنّ الخط أو الإمضاء أو الختم أو البصمة هي لمن تلقى عنه الحق. ومن احتجّ عليه بمحرر عرفي وناقش موضوعه، لا يقبل منه إنكار الخط أو الإمضاء أو الختم أو بصمة الإصبع، و"لا يكون المحرر العرفي حجة على الغير في تاريخه إلا منذ أن يكون له تاريخ ثابت، ويكون للمحرر تاريخ ثابت من يوم أن يقيد بالسجل المعدّ لذلك، ومن يوم أن يثبت مضمونه في ورقه أخرى ثابتة التاريخ، ومن يوم أن يؤشر عليه موظف عامّ مختصّ، ومن يوم وفاة أحد ممن لهم على المحرر أثر معترف به من خط أو إمضاء أو بصمة أو من يوم يصبح مستحيلاً على أحد من هؤلاء أن يكتب أو يبصم لعلة في جسمه، ومن يوم وقوع أيّ حادث آخر يكون قاطعًا في أن الورقة قد صدرت قبل

1 المواد (11، 14، 15) من قانون قانون الإثبات في المواد المدنية والتجارية المصري رقم 1968/25.

وقوعه، ومع ذلك يجوز للقاضي تبعًا للظروف ألاّ يطبق حكم هذه المادة على المخالصات.

ونصّ قانون المعاملات الإلكترونية البحريني على أنه "للسجلات الإلكترونية ذات الحجية المعتمدة، الإثبات للمحررات العرفية، ولا ينكر الأثر القانوني للمعلومات الواردة في السجلات الإلكترونية، من حيث صحّتها وإمكان العمل بمقتضاها، لمجرد ورودها -كلّيًا أو جزئيًا- في شكل سجل إلكتروني أو الإشارة إليها في هذا السجل[1].

"لا ينكر الأثر القانوني للتوقيع الإلكتروني، من حيث صحته وإمكان العمل بموجبه، لمجرد وروده -كلّيًا أو جزئيًا- في شكل إلكتروني إذا لم يتم وضع التوقيع الإلكتروني باستعمال شهادة معتمدة، فإنّ قرينة الصحة المقرّرة بموجب أحكام البند السابق لا تلحق أيًا من التوقيع أو السجل الإلكتروني[2]".

وهو الأمر الذي لم يخرج به القانون البحريني عن نفس الآثار المقررة للتوقيع الإلكتروني التي قررتها القوانين العربية الأخرى آنفة الذكر[3].

وبعد هذا العرض فإننا نخلص إلى أنّ وجود التوقيع الإلكتروني ضمن المحرر على وسيط إلكتروني غير مادي وانفصاله عن شخص الموقع قد يثير الشك حول مصداقيته في تمييز هوية صاحبه وضمان ارتباطه بالتصرف القانوني، حيث يمكن للقراصنة اختراق نظام المعلومات ومعرفة التوقيع وفك شفرته واستخدامه دون

---

1 المادة (5) القانون رقم 2002/28 بشأن المعاملات الإلكترونية.

2 المادة (6) القانون رقم 2002/28 بشأن المعاملات الإلكترونية.

3 مجدي أحمد عزام، الحجية القانونية للتوقيع الإلكتروني والمعاملات الإلكترونية في القوانين العربية "دراسة مقارنة"، مرجع سابق.

موافقة صاحبه، كلّ ذلك بخلاف التوقيع العادي الذي يتطلب الحضور الجسماني لصاحبه، ممّا يسهّل التحقّق منه، ويتم الاحتفاظ بنسخة من المحرر تكون بمنأى عن العبث والتغيير، ويمكن لخبراء الخطوط كشف أيّ تلاعب أو تزوير في التوقيع، وإنّ مثل هذا التخوّف رغم ما ينطوي عليه من بعض الصواب لم يقف عقبة أمام استخدام الوسائل التكنولوجية الحديثة في مجال الإثبات(1).

وهذا بالاستعانة بجهات التوثيق الإلكترونية والمرخص لها القيام بهذه الوظيفة، حيث تقوم بمنح شهادات بصحة التوقيع الإلكتروني، وذلك بعد التحقّق من شخصية الأطراف المتعاقدة واتّباع وسائل الأمان التقنية التي تضفي حماية وسرية لهذا التوقيع(2).

ونخلص ممّا سبق، وبما أنّ التوقيع الإلكتروني أثبت قدرته على أداء مهام التوقيع الكتابي التقليدي، فإنّ المشرع قد اعتمد هذا التوقيع الإلكتروني، ومنحه القوة الثبوتية أمام المحاكم، والجهات الحكومية، ومنح المستندات الإلكترونية القوة الممنوحة للمستندات الورقية التقليدية، إذ أصبح هذا واقعًا لا مفرّ منه في ظلّ التطورات الحالية في المعاملات التجارية الدولية عبر شبكة الإنترنت، وهذا ما جعل الاعتراف بالتوقيع الإلكتروني والمستندات الإلكترونية مسألة ضرورية بما يمكن الأطراف المتعاقدة من تقديم المستندات بعد استخراجها من الحاسب الآلي وتوقيعها إلكترونيًّا، وعدّها أدلة للإثبات تقدّم إلى الجهات القضائية.

---

1 محمد حسين منصور، المسؤولية الإلكترونية، مرجع سابق، ص 287.

2 سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، 2007م، ص 23.

الخاتمة

وسأذكر فيها النتائج والتوصيات التي تم التوصل إليها:

النتائج:

1. يعتبر التوقيع الإلكتروني ضمانة حقيقية ظهرت وتوسّع في استخدامها ترتيبًا على التوسع في استخدام الحاسب الآلي، وتقدم تطبيقاته وتقنياته على نحو جعل الحياة اليومية للأفراد والدول تعتمد عليه بصفة شبه كلية.
2. إنّ التوقيع الإلكتروني هو إجراء معيّن يقوم به الشخص المراد توقيعه على المحرر بغض النظر عن شكله سواء أكان رقمًا أم شفرةً معيّنةً، ممّا يحفظ السرية ويعطي الثقة في دلالة التوقيع على صاحبه.
3. يعتبر التوقيع من المبادئ الأساسية في الإثبات وشرطًا مهمًّا لتوثيق أيّ مستند سواء في المراسلات العادية أم الإلكترونية على اختلاف أنواعها ووسائطها في داخل المؤسسة أو المراسلات التي تتم بين المؤسسات في داخل الدولة أو خارجها.
4. يساهم التوقيع في فتح قناة اتصال جديدة بين المواطن والجهات الحكومية يمكن من خلالها النفاذ إلى مستويات الإدارة العليا لزيادة الشفافية في الأعمال الحكومية، وبالتالي يعدّ عاملاً وأداةً مهمة لنجاح فكرة الحكومة الإلكترونية.
5. إنّ قانون التجارة الإلكترونية الإماراتي جرم –تزويـــر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة نشاط من الهيئة– حماية للتوقيع

الإلكتروني من خلال إنشاء شهادة تتضمّن بيانات غير صحيحة، مع العلم بذلك أو نشرها أو تقديمها لأيّ غرض غير مشروع.

6. إنّ التشفير إجراء يؤدّي إلى توفير الثقة في المعاملات الإلكترونية، وذلك باستخدام أدوات أو أساليب لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها غير المشروع.

7. لكي يكون التوقيع الإلكتروني ضمانة حقيقية لأطراف المعاملة الإلكترونية يجب أن يكون مصدّقًا، حيث يعتبر التصديق أحد الضمانات القانونية لإثبات صحة التوقيع الإلكتروني، وبالتالي صحة المعاملات الإلكترونية.

8. إنّ جهات التوثيق والتصديق الإلكتروني تعدّ الشخص المسؤول عن إصدار شهادة تتضمّن تحديد هوية الموقع وتثبيت صلتة بالتوقيع الإلكتروني، ولولا وجود هذا الشخص لأحجم الكثير من المتعاملين عن الأقدام على التعامل القانوني الإلكتروني.

9. إنّ الهدف من شهادة التصديق تأكيد صحة وقانونية البيانات الواردة في الشهادة، كما تؤكّد لنا صحة وقانونية التوقيع الإلكتروني.

10. حتى يتمتّع التوقيع الإلكتروني بحجية في الإثبات لا بد أن يستوفي الشروط التي تمنحه الحجية القانونية في الإثبات، والتي يؤدّي عدم توافرها إلى عدم تحقّق وصف التوقيع الإلكتروني، وذلك من خلال تحديد هوية الموقِع، والتأكّد من صحة التوقيع وصلاحيته للاحتجاج به قانونًا، كونه يعبّر عن إرادة الأطراف في التصرف.

11. إنّ الغرض من إجراءات التوثيق هو التحقق من أنّ التوقيع الإلكتروني لم يتعرض إلى التعديل أو التغيير، وهو ما يؤدّي إلى إعطاء التوقيع الإلكتروني الحجية القانونية في مواجهة أطرافه والغير.
12. إنّ من أهمّ تطبيقات التوقيع الإلكتروني البطاقات البلاستيكية، التلكس، الشيك الإلكتروني وسند الشحن الإلكتروني وغيرها.
13. إنّ الاعتراف بالتوقيع الإلكتروني والمستندات الإلكترونية مسألة ضرورية بما يمكّن الأطراف المتعاقدة من تقديم المستندات بعد استخراجها من الحاسب الآلي وتوقيعها إلكترونيًّا، وعدّها أدلة للإثبات تقدّم إلى الجهات القضائية.
14. أعطى القانون الإماراتي للمحررات الإلكترونية والكتابة الإلكترونية والتوقيع الإلكتروني نفس الحجية المقررة للتوقيعات والمحررات المذكورة في قانون الإثبات في المعاملات المدنية والتجارية متى استوفت الشروط والأحكام المقرّرة في قانون المعاملات والتجارة الإلكترونية.
15. إنّ المشرع الإماراتي قد أعطى ذات الحجية للتوقيع الإلكتروني التي أعطاها للتوقيع التقليدي، وبذلك يكون المشرع الإماراتي قد خطا خطوات مهمّة نحو التجارة الإلكترونية وتدعيمها.

التوصيات:

1. ضرورة إدخال موظّفي الجهات ذات العلاقة المباشرة بالتوقيع الإلكتروني في دورات تأهيلية تمكّنهم من التعامل مع تلك الوسائل المستحدثة.
2. ضرورة أن تلاءم التشريعات العربية ما سارت عليه التشريعات في الدول الأخرى، وبخاصة قانون الأونسيترال النموذجي.
3. ضرورة إنشاء أجهزة ومرافق عامة تأخذ على عاتقها مهمّة القيام ووضع آليات وقواعد حفظ المحررات الإلكترونية.
4. ضرورة تصدّي المشرّعين إلى مسألة تحديد مكان انعقاد التصرفات الإلكترونية والعقود الإلكترونية ووقتها.
5. ضرورة تحديد جهات تصديق التوقيعات والمحررات الإلكترونية والمحافظة على البيانات والمعلومات الشخصية وحمايتها من الإفشاء وترتيب مسؤولية مدنية وجزائية على ذلك.
6. ضرورة عدم تبني المشرع تقنية توقيع إلكتروني معينة للاعتراف بها دون غيرها، فقد تظهر مستقبلاً حاجة لتعديل هذه النصوص بما يتفق مع التطورات التقنية الحديثة.
7. العمل على إصدار معاهدة عربية دولية تنصّ على أحكام مشتركة للتوقيع الإلكتروني من حيث شروطه وكيفية استخدامه وحجيته في الإثبات ووسائل حمايته وآثاره، ومنازعاته أمام القضاء باعتبار أن التوقيع الإلكتروني من الأمور غير المحلية بل من الأمور الدولية.

قائمة المصادر والمراجع

أولاً: المراجع (الكتب العامة)

1. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، الكويت، 2003م.
2. إيمان مأمون أحمد، الجوانب القانونية لعقد التجارة الإلكترونية، القاهرة، دار النهضة العربية، 2005م.
3. إلياس أبو عبيد، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، الجزء الأول، منشورات الحلبي الحقوقية، 2005م.
4. بشار محمود دودين، الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، دار الثقافة، للنشر والتوزيع، ط 2، 2010م.
5. تامر محمد عبد الباقي الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت: دراسة مقارنة، منشأة المعارف، 2009م.
6. جميل عبد الباقي، الحماية الجنائية التهامي، لبطاقات الائتمان الممغنطة. دار النهضة العربية. دار النهضة، القاهرة، 2003م.
7. حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2000م.
8. رأفت رضوان، عالم التجارة الإلكترونية، منشورات المنظمة العربية للعلوم الإدارية، القاهرة 1999م.
9. سامح عبد الواحد التهامي، التعاقد عبر الإنترنت، دار الكتب القانونية، مصر، 2008م.
10. سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، 2007م.

11. طاهر شوقي مؤمن، عقد البيع الإلكتروني، بحث في التجارة الإلكترونية، دار النهضة العربية، القاهرة، 2007م.
12. عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنت، دار الكتب القانونية، مصر، 2008م.
13. عبد الفتاح بيومي حجازي، مقدمة في التجارة العربية الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، 2003م.
14. عبد الفتاح بيومي، "النظام القانوني لحماية التجارة الإلكترونية"، الطبعة الأولى دار الفكر العربي، 2002م.
15. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، المحلة الكبري، مصر: دار الكتب القانونية: دار شتات للنشر، 2007م.
16. فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة للنشر، مصر، 2002م.
17. لورنس محمد عبيدات، إثبات المحرر الإلكتروني، الطبعة الأولى، عمان: دار الثقافة للنشر والتوزيع، 2005م.
18. محمد السعيد رشدي، التعاقد بوسائل الاتصال الحديثة ومدى حجيتها في الإثبات، منشأة المعارف، الإسكندرية، 2008م.
19. محمد خالد جمال رستم، التنظيم القانوني للتجارة والاثبات الإلكتروني في العالم، منشورات الحلبي الحقوقية، بيروت، 2006م.
20. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية، القاهرة، 2009م.
21. محمد فواز المبرهم، الوجيز في عقود التجارة الإلكترونية (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2005م.

22. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، 2001م.
23. مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الإنترنت، دار الكتب القانونية، مصر، 2010م.
24. نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2005م.
25. وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، لعام 2007م.

ثانيًا: المراجع (الكتب المتخصّصة)

1. آزاد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2015م.
2. أسامة روبي عبد العزيز الروبي، حجية التوقيع الإلكتروني في الإثبات والادعاء مدنيًا بتزويره وفقًا لقانوني الإثبات والمعاملات الإلكترونية العمانيين دراسة مقارنة بالقانونين المصري والفرنسي، دار النهضة العربية، 2010م.
3. الأستاذ. منير محمد الجنبيهي، الأستاذ. ممدوح محمد يوسف الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، 2008م.
4. أمير فرج يوسف، الجديد في التوقيع الإلكتروني لدول الخليج العربي والحجية القانونية للتوقيع الإلكتروني في كافة المعاملات الإلكترونية، دراسة قانونية مقارنة بالدول العربية والأجنبية، دار الكتب والدراسات العربية، الإسكندرية، 2015م.
5. أيمن سعد حسين، التوقيع الإلكتروني دراسة مقارنة، دار النهضة العربية، 2013م.

6. أيمن علي حسين، التوقيع الإلكتروني بين النظرية والتطبيق، دار المطبوعات الجامعية، 2011م.
7. عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة المكتب الجامعي الحديث، الإسكندرية، 2009م.
8. عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، بيروت، لبنان، ط 1، 2010م.
9. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، 2005م.
10. علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر والتوزيع، عمان الأردن، 2005م.
11. عمر حسن المومني، التوقيع الإلكتروني والتجارة الإلكترونية، الطبعة الأولى، دار وائل للنشر، عمان، الأردن، 2003م.
12. عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة لنشر والتوزيع، الطبعة الأولى، 2009م.
13. فيصل سعيد الرومي، التوقيع الإلكتروني وحجيته في الإثبات، المنظمة العربية للتنمية الإدارية، 2005م.
14. قدري عبد الفتاح الشهاوي، قانون التوقيع الإلكتروني ولائحته التنفيذية والتجارة الإلكترونية في التشريع المصري والعربي والأجنبي، دار النهضة العربية، مصر، 2005م.
15. المحامية عبير ميخائيل الصفدي الطوال، التوقيع الإلكتروني، دار وائل للنشر والتوزيع، عمان- الأردن، ط 1، 2010م.

16. محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2006م.
17. محمد حسن قاسم، أصول الإثبات في المواد المدنية والتجارية، منشورات الحلبي الحقوقية، بيروت، لبنان، بدون سنة طبع.
18. المستشار الدكتور محمد الشهاوي، شرح قانون التوقيع الإلكتروني رقم (15) لسنة 2004 دراسة مقارنة، الطبعة الأولى، 2010م.
19. خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني، دار الجامعة العربية، القاهرة، 2007م.
20. تامر محمد عبد الباقي الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت، دراسة مقارنة، منشأة المعارف، 2009م.
21. خالد ممدوح إبراهيم، أبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية عام 2006م.
22. سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، 2007م.
23. سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته ـ صورة ـ حجيته في الإثبات بين التدويل والاقتباس، دار الجامعة الجديدة عام 2004م، الإسكندرية.

ثالثًا: الرسائل العلمية

أطاريح الدكتوراه:

1. براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم تخصص قانون جنائي، جامعة محمد خضير بسكرة، الجزائر، 2015م.
2. هادي مسلم يونس قاسم البشكاني، التنظيم القانوني للتجارة الإلكترونية، دراسة مقارنة، أطروحة دكتوراه مقدمة إلى مجلس كلية القانون في جامعة الموصل، 2002م.
3. عايض راشد عايض المري، مدى حجية الوسائل التكنولوجية الحديثة في آليات العقود التجارية، رسالة دكتوراه 1998م، غير منشورة، جامعة القاهرة.

رسائل الماجستير:

1. حسون علي حسون، التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة ماجستير، مقدمة إلى كلية القانون، جامعة بابل، 2006م.
2. يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات وفقًا لقانوني الإثبات والمعاملات الإلكترونية الأردنيين، رسالة ماجستير غير منشورة، الجامعة الأردنية، عمان، الأردن، 2005م.

رابعًا: البحوث والندوات والمؤتمرات

1. إيناس الخالدي، حجية التوقيع الإلكتروني في الإثبات دراسة في نظام التعاملات الإلكترونية السعودي، كلية الدراسات القضائية والأنظمة، جامعة أم القرى.
2. باسيل يوسف، الاعتراف القانوني بالسندات والتواقيع الإلكترونية في التشريعات المقارنة، بحث منشور في مجلة دراسات قانونية، بيت الحكمة، بغداد، العدد الرابع، 2000م.

3. حسن زرادني، "حجية التوقيع الإلكتروني في ضوء القانون 53.05"، أشغال الندوة العلمية المنظمة بالكلية المتعددة التخصصات بآسفي، تحت عنوان القانون الإلكتروني وحماية المعلومات، غير منشور.
4. عبد العزيز المرسي حمود، مدى حجية المحرر الإلكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافذة، بحث منشور في مجلة البحوث القانونية والاقتصادية، كلية الحقوق بجامعة القاهرة، العدد 11، السنة11، أبريل، 2002م.
5. عمر يونس، قانون اليونسترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996م، المؤتمر الدولي الأول لقانون الإنترنت، ورشة عمل نحو علاقات قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة، المنظمة العربية للتنمية الإدارية، منظمة الدول العربية، الغردقة، جمهورية مصر العربية، 2005م.
6. محمد المرسي زهرة، مدي حجية التوقيع الإلكتروني في الإثبات، مؤتمر الكمبيوتر والقانون –كلية الحقوق– جامعة عين شمس– فبراير، 1994م.
7. غازي أبو عرابي، فياض القضاة، "حجية التوقيع الإلكتروني"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الأول 2012م، بحث منشور.

خامسًا: الصحف والمجلات

1. أسامة بن غانم العبيدي، "حجية التوقيع الإلكتروني"، المجلة العربية للدراسات الأمنية والتدريب، العدد 56، ب. ت.
2. بدر القحطاني، جريدة الشرق الأوسط، 14/ 5/ 2010 م، العدد 1149.
3. عبد الحميد، رائد، مجلة العدالة والقانون، مدى حجية وسائل الاتصال الحديثة في قانون البينات، العدد (2)، يوليو، سنة 2005م، رام الله.

4. عبد الرسول عبد الرضا، محمد جعفر هادي، المفهوم القانوني للتوقيع الإلكتروني، دراسة مقارنة، مجلة المحقق الحلي للعلوم القانونية والسياسية العدد الأول/ السنة الرابعة.
5. قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012، منشور في مجلة الوقائع العراقية بالعدد 4274 في 15/ 4/ 2013م.
6. مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثالث، السنة السابعة، 2015م.
7. مجلة نقابة المحامين الأردنيين، العدد الصادر سنة (1987) على الصفحة رقم 3/1884 قرار تميز رقم (619).
8. أ. محمد بودالي، التوقيع الإلكتروني، مجلة الإدارة، العدد رقم 2، لسنة 2003.
9. محمود ثابت محمود، حجية التوقيع الإلكتروني في الإثبات، مجلة المحاماة، العدد الثاني، 2002م.
10. نور الدين الناصري، المعاملات الإلكترونية في ضوء القانون رقم 53/05 المتعلق بالتبادل الإلكتروني للمعطيات، مجلة القانون الاقتصادي العدد الثاني، يناير 2009م، مطبوعات الهلال، وجدة، المغرب.

سادسًا: القوانين والاتفاقيات والأحكام

1. القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية.
2. القانون الاتحادي رقم 2006/36.
3. قانون الإثبات في المواد المدنية والتجارية المصري رقم (8) لسنة 1976.
4. قانون الأحوال الشخصية الأردني المعدل رقم (61) لسنة 1976.
5. القانون الأردني للمعاملات الإلكترونية رقم (85) لسنة 2001.

6. قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.
7. القانون الفرنسي لتنظيم الاتصالات عن بعد رقم (90) لسنة 1990 والمعدل بموجب القانون رقم (575) لسنة 2004.
8. قانون المبادلات والتجارة الإلكترونية التونسي رقم (83) لسنة 2000.
9. القانون المتعلق بالتبادل الإلكتروني للمعطيات القانونية المغربية رقم 53.05.
10. القانون المصري للتوقيع الإلكتروني رقم 15 لسنة 2004.
11. قانون المعاملات والتجارة الإلكترونية دبي رقم (2) لسنة 2002.
12. قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012.
13. قانون تصديق اتفاقية تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية رقم (101) لسنة 2012.
14. قانون مملكة البحرين بشأن المعاملات الإلكترونية رقم (28) لسنة 2002.
15. قرار وزير الاتصالات وتكنولوجيا المعلومات المصري رقم (109) لسنة 2005.
16. اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم (15) لسنة 2004.
17. نظام التعاملات الإلكترونية السعودي رقم (80) وتاريخ 7/ 3/ 1428 هـ.

سابعًا: مواقع الإنترنت

1. الجرائم الواقعة على التجارة الإلكترونية، بقلم الدكتور: حسين بن سعيد بن سيف الغافري، سلطنة عمان مسقط، 2006م، منشور على الموقع الإلكتروني، تاريخ الزيارة 2016/12/1م.

http://www.mohamoon.com/montada/Default.aspx?Action=Display&ID=106198&Type=3

2. أحمد السيد كردي، "التوقيع الإلكتروني مفهومه التكنولوجي وحمايته"، تاريخ الاطلاع 2016/12/1م.

http://kenanaonline.com/users/ahmedkordy/topics/68795#http://kenanaonline.com/users/ahmedkordy/posts/323677

3. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، منشور على الموقع الإلكتروني http://www.startimes.com/?t=17717139 تاريخ الاطلاع: 14-02-2017م.

4. خالد ممدوح إبراهيم، الشكلية في عقود الإنترنت والتجارة الإلكترونية، منشور على الموقع الإلكتروني، تاريخ الاطلاع عليه: 20-2-2017م.

ttp://kenanaonline.com/users/KhaledMamdouh/posts/77862

5. مجدي أحمد عزام، المحامي بالنقض والإدارية العليا محاضر بمعهد المحاماة بالإسكندرية دراسات عليا في القانون صاحب إصدارات قانونية مسجلة بدار الكتب، منتدى المحامين العرب المنتدى العام بحث عن الحجية القانونية للتوقيع الإلكتروني والمعاملات الإلكترونية في القوانين العربية "دراسة مقارنة" منشور على الموقع الإلكتروني تاريخ الاطلاع عليه: 20-2-2017م.

http://www.mohamoon.com/MONTADA/Default.aspx?Action=Display&ID=117932&Type=3

6. أسامة بن غانم العبيدي، حجية التوقيع الإلكتروني في الإثبات، منشور على الموقع الإلكتروني:

dar،www.nauss.edu.sa/Ar/CollegesAndCenters/.../1434/.../em، 56،4.pdf ، تم الاطلاع عليه بتاريخ: 14-02-2017م.

ثامناً: المراجع باللغة الأجنبية

1. European Council Directive 2000/31/EC، 2000 O.J. (L .178) 1-12 See Article (5) ، Council Directive ، Id. at 8.
2. Anthony، Burke، EU and Irish Internet Law An Overview، 13 Int'l L. Practicum، at 107، 113 15 (Autumn 2000).
3. Jacqueline، Klosek (2000): EU Telecom Ministers Approve Electronic Signatures .Directive، 4 Cyberspace Law 12.
4. Council Directive 1999/93/FC ، 2000/31/EC، 2000 O.J. (L .178) 1-12
5. Id..at 11، Annex 11 (d) See also Council Derective ، Supra، at 7 ، art.
6. Klosek، Jacqueline، EU Telecom Ministers Approve Electronic Signatures Supra. 12. Directive ،United National Commission on International Trade Law، UNC، ITRAL Law on Electronic Commerce With Guide to Enactment (1996) ، at http: // www.uncitral.org/ English / texts / telecom / ml. htm.
7. UNCITRAL Model Law on Electronic Signatures، (2001) 32 Y.B. U.N. CommissionInt'l Trade L. 499، U.N Doc. A/CN.9/SER.A/2001.
8. Draft Guide to Enactment of UNCITRAL Model law on Electronic Signatures :Note by the Sceretatiat، U.N .GAOR، 34th Sess. ، at

17-18 ، cmt. 32. U.N. Doc.A/CN.9/493 (2001) ، reprinted in (2001) 32 Y.B. U.N. Commission Int'l Trade L.313، 321-22 ، Cmt. 32، U.N. Doc. A.CN. 9/SER. A/ 2001.

9. European Union Electronic Commerce Directive، 1999/93/EC.
10. 1BBC News، Business، Digital Signature becomes Law، at : http://news.bbc.co.uk/2/hi/business/1446426 .
11. PNC Telecom V. Thomas (2002) EWHC 284 (Ch).
12. BBC news،Clinton Oks ،e-signatures at http://news.bbc.co.uk/2hi/science/nature/813437.stn.
13. Ian A. Rambarran، I Accept But Do They? : The Need for Electronic Signature Legislation on Mainland China، 15 TRANSNAT'L Law 405، 417-18، (2002) .
14. UNIF. ELEC. TRANSACTIONS Act، 7A U.L.A.23 (2002 and supp.. 2004) See also Christopher William Pappas، Comparative U.S and EU Approaches to Ecommerce Regulations : Jurisdiction، Electronic Contracts، Electconic Signatures and Taxation، 31 DENV. J. INT.LL and Poly 325، 341 (2002).
15. UNIF. ELEC. TRANACTIONS Act، 7A U.L.A.252، 2002.
16. Electronic Signatures in Global and National Commerce Act. 15 U. S.C. *ff* 7001 .(2000).
17. Amy J. Dunn، Survey of Legislation: Uniform Electronic Transactions، 24 U، (2000).